

现代应用数学丛书

# 代 数 学

〔日〕弥永昌吉 杉浦光夫 著

上海科学技术出版社

51.43  
340

現代应用数学丛书

# 代 数 学

〔日〕 彌永昌吉 著  
杉浦光夫  
熊 全 淹 譯

上海科学技术出版社



## 內 容 提 要

本书是日本岩波书店出版的现代应用数学丛书之一的中译本。全书共分三章,包括线性代数、群论基础、Boole 代数、有限体理论初步和有限群表现论。最后,为便于读者对有限群表现论的了解,另节译了 H. Zassenhaus: Lehrbuch der Gruppen theorie 一书中“有限旋转群”部分作为附录。本书可供高等院校数学系、物理系师生作参考。

现代应用数学丛书

## 代 数 学

原 书 名 代 数 学

原 著 者 (日) 彌永昌吉  
杉浦光夫

原出版者 岩波书店 1957

译 者 熊 全 淹

\*

上海科学技术出版社出版

(上海瑞金二路450号)

上海市书刊出版业营业登记证出 093 号

新华书店上海发行所发行 各地新华书店经售

商务印书馆上海厂印刷

\*

开本 850×1168 1/32 印张 9 16/32 字数 225,000

1962 年 11 月第 1 版 1962 年 11 月第 1 次印刷

印数 1—5,500

统一书号: 13119 · 484

定 价: (十四) 1.60 元

## 出版說明

这一套书是根据日本岩波书店出版的“現代应用数学讲座”翻譯而成。日文原书共15卷60册，分成A、B两组，各編有序号。現在把原来同一題目分成两册或三册的加以合并，整理成42种，不另分組編号，陸續翻譯出版。

这套书涉及的面很广，其內容都和現代科学技术密切有关，有一定参考价值。每一本书收集的資料都比較丰富，而叙述扼要，篇幅不多，有利于讀者以較短時間掌握有关学科的主要內容。虽然，这套书的某些观点不尽适合于我国的情况，但其方法可供参考。因此，翻譯出版这一套书，对我国学术界是有所助益的。

由于日文原书是1957年起以讲座形式陸續出版的，写作時間和篇幅的限制不可避免地会影响原作者对內容的处理，为了尽可能地减少这种影响，我們在每一譯本中，特請譯者或校閱者撰写序或后記，以介紹有关学科的最近发展状况，并对全书內容作一些評价，提出一些看法，結合我国情况补充一些資料文献，在文內过于簡略或不足的地方添加了必要的注釋和改正原书中存在的一些錯誤。希望这些工作能对讀者有所帮助。

承担翻譯和校閱的同志，为提高书籍的质量付出了巨大劳动，在此特致以誠摯的謝意。

欢迎讀者对本书提出批評和意見。

上海科学技术出版社

## 現代应用数学丛书

书 名	原作者	譯 者	书 名	原作者	譯 者
代 数 学	弥永昌吉等	熊全淹	非綫性振动論	古 屋 茂	呂紹明
几 何 学*	矢野健太郎	孙澤瀛	力学系与論*	岩 田 义 一	孙澤瀛
复 变 函 数	功力金二郎	刘书琴	平面彈性論*	森 口 繁 一	刘亦珩
集合·拓朴·測度*	河 田 敏 义	賴英华	有限变位彈性論*	山 本 善 之 大	刘亦珩
泛 函 分 析*	吉 田 耕 作	程其襄	变 形 几 何 学*	近 藤 一 夫	刘亦珩
广 义 函 数*	岩 村 联	楊永芳	塑 性 論*	鷗 津 文 一 郎	刘亦珩
常 微 分 方 程	福原滿洲雄	張庆芳	粘性流体理論*	谷 一 郎	刘亦珩
偏 微 分 方 程*	南 云 道 夫	錢端仕	可压缩流体理論*	河 村 龙 馬	刘亦珩
特 殊 函 数*	小谷正雄等	錢端仕	网 絡 理 論	喜安善市等	陆志刚
差 分 方 程	福 田 武 雄	穆鴻基	自 动 控 制 論	喜安善市等	程立林
富里哀变换与拉普拉斯变换*	河 田 龙 夫	錢端仕	回 路 拓 扑 学	近 藤 一 夫	張鳴鏞
变分法及其应用*	加 藤 敏 夫	周怀生	信 息 論	喜安善市等	李文清
李 群 論*	岩 堀 长 庆	孙澤瀛	推 断 統 計 理 論	北 川 敏 男	李賢平
随 机 过 程*	伊 藤 清	刘璋温	統 計 分 析*	森 口 繁 一	刘璋温
同 轉 群 与 对 称 群 的 应 用	山 内 恭 彦 等	張质賢	实 驗 設 計	增 山 元 三 郎	刘璋温
結晶統計与代数	伏 見 康 治	孙澤瀛	群 体 遺 傳 学 的 理 論*	木 村 資 生	刘祖潤
偏 微 分 方 程 的 应 用	犬 井 鉄 郎 等	楊永芳	博 奕 論	官 澤 光 一	張毓春
微 分 方 程 的 近 似 解 法	加 藤 敏 夫 等	王占瀛	綫 性 規 划	森 口 繁 一	刘源張
数 值 計 算 法	森 口 繁 一 等	閻昌齡	經 济 理 論 中 的 数 学 方 法	安 井 琢 磨 等	談祥柏
量 子 力 学 中 的 数 学 方 法*	胡 永 振 一 郎	周民强	随 机 过 程 的 应 用*	河 田 龙 夫	刘璋温
工 程 力 学 系 統*	近 藤 一 夫 等	刘亦珩	計 算 技 术	高 桥 秀 俊	姚 晋
			穿 孔 卡 計 算 机	森 口 繁 一	刘源張

注：有 \* 者已在 1962 年 7 月以前出版。

## 譯 者 序

本书共三章，所叙述的都是代数中主要的并且是应用广泛的部分，重点在第3章，而以第1章及第2章中的群为其基础。当然第1章綫性代数也是应用极为广泛的。

本书篇幅虽然不多，但内容丰富，由于取材适宜，安排恰当，所以重点突出，有条不紊。全书立足点高，抽象性强，论证严，对基本概念的阐述和重要定理的证明力求详尽，有些较复杂的对应关系则另用图式说明，使读者易于理解。有些重要定理及公式在文中顺便引出而不另加证明，使在不模糊重点之下，又便于读者得窥全貌，这些都是本书之长。此外，例题丰富更为他书所不及，很多重要性质是通过例题来给出，主要演算亦借例题来说明，其重要不在系及命题之下，读者不可轻易放过。遗憾的是例题中的推导和演算有时过于简略，初读者不容易理解。尽管如此，本书的确是一本好书，尤其对应用数学者不可多得，是值得介绍。

第1章綫性代数，先述向量空间的基本概念及主要性质，次述Jordan标准形，最后叙述二次形式及Hermite形式，举凡綫性代数方面的主要理论及基本演算方法大部均已具备。全部理论建立在映射这个概念之上，其中一再引用到§8的用矩阵表现映射的结果，希望读者注意。第2章介绍群，Boole代数，有限体，简单明了，似都容易领会，不必再加解说。兹仅就本书主要部分第3章有限群的表现论，详细说明如下。

在§25, 26, 27, 28等节中讲述群表现，表现空间，不变子空间，可约及既约表现等基本概念以及在群表现论中起重要作用的基本定理：Schur引理，并证明了在具有内积的向量空间中有限

群的任意表現是完全可約的。

在 § 29, 30 中給出群代數的定義, 由它得到有限群的具体表現, 即正則表現与伴隨表現。

在 § 31 中, 首先引用 Schur 引理推出既約表現的矩陣元素間的直交关系, 由此导出 Burnside 定理, 然后在 § 32 中引入群的特征標概念, 利用特征標的性质判別两个表現是否等价。在 § 33 中討論了群代數的构造問題, 利用特征標的直交关系指出有限群的既約表現都在正則表現中出現。証明了群代數与矩陣环的直和同构, 引入群代數的中心与类函数的概念, 因而推得了群的既約表現 (不等价的) 的个数等于群的共轭类的个数, 最后給出了計算 3, 4 阶对称群特征標的实际例子。

§ 34 中讲述群的直积表現, 特別討論了有限可換群的直积分解及可換群与其特征標群的同构。§ 35 叙述由子群的表現构造群的表現的方法, 誘導表現即是由一个群的子群的已知表現誘導出这个群的表現, 并討論了关于誘導表現的 Frobenius 的相互律。

§ 36 进一步討論群特征標的性质, 并引用代數整數論的知識与特征標的直交关系証明了既約表現的級数是群的阶数的約数, 并給出类函数成为單純特征標的必要充分条件。

§ 37 繼續討論群代數的构造, 引入兩側理想, 最小左(右)理想, 幂等元与既約幂等元等概念, 指出既約幂等元, 最小左(右)理想与既約表現的关系, 給出两个既約幂等元等价的必要充分条件。最后証明群代數的理想的直和分解。

在 § 38, 39, 40, 41 等节中, 詳細討論了对称群的表現理論。首先引入 Young 台及它的 Young 对称子, 指出了对称子是既約幂等元, 以及两个对称子等价的必要充分条件是它們同在一个 Young 的台中, 以后又引入标准台的概念, 由此証明对称群的阶数是既約表現 (不等价的) 級数的平方和, 并举出了构造对称群表

現的实际方法。

§ 42, 43 两节介绍 Weyl 关于  $n$  阶对称群  $G$  与  $m$  维向量空间  $V$  上一般线性变换群  $GL(V)$  在直积空间  $V^n$  中的  $n$  级直积表现关系, 指出直接表现是完全可约的, 并且它所含的既约表现(不等价的)与行数小于或等于  $m$  的 Young 的台一一对应, 其中每个既约表现的重复度等于上述所对应的 Young 的台的标准台的个数。

这章内容已如上述。整个理论的建立是以群代数为基础, 并将群代数看成为群上的函数环(即定义域是群的一切函数所构成的环), 从而导出了群的正则表示, 以及把表现矩阵中的元素看成为群上函数而导出了 Burnside 定理, 视特征标为类函数而建立起特征标的理论等等。在对称群的表现理论与 Weyl 理论的讨论中也无时不引用群代数。因此, 除 § 25, 26, 27 中所述的一些基本概念之外, § 29, 33, 37 等节中有关群代数的定义和定理的部分都是相当重要的, 因为这些概念和理论不仅是有限群表现论的基础, 并且在无限群的表现论中也有重要意义。

特别是对于对称群的表现论, 这章取材丰富, 叙述详尽, 在现行的群表现论书籍中还不多见。

最后, 由于一般线性变换群含有直交变换群, 酉变换群等其他特殊线性变换群, 因此它的直积表现论, 在群的理论研究中非常重要。另一方面, 这个理论在量子力学的多粒子问题中也有重要应用, 后面介绍了 Weyl 在这方面的成果。Weyl 的原著(Classical group)叙述得不够清楚, 艰涩难读, 经过本书整理, 特别是在群代数的观点下来详细论证, 就比原著清楚易读了。这对需要这方面理论的读者将是有益的。

在本书翻译过程中, 就译者认为较难理解的地方作了一些注解, 希望能对初读者有所帮助。但由于水平所限, 挂一漏万以及错



誤之處在所難免，請讀者批評指正。譯稿承管紀文同志，曹和貴同志校閱，提出了很多寶貴意見，此外曹和貴同志又添補了很多注解（特別在第3章），謹此一一致謝。

熊 全 淹 1961 年 9 月

# 目 录

出版說明

譯者序

第 1 章	綫性代数 .....	1
§ 1	向量及綫性运算 .....	1
§ 2	关于現代代数学的方法 .....	5
§ 3	作为代数系的向量空間 .....	6
§ 4	子空間,生成元,直和分解 .....	11
§ 5	綫性无关,綫性相关,維数,基底 .....	19
§ 6	关于映射 .....	24
§ 7	綫性映射 .....	28
§ 8	矩陣表現 .....	34
§ 9	秩与退化次数 .....	43
§ 10	对偶空間与轉置映射 .....	47
§ 11	1 次方程 .....	52
§ 12	行列式 .....	57
§ 13	綫性变换及其不变子空間 .....	69
§ 14	特征值,特征多项式, Cayley-Hamilton 定理 .....	72
§ 15	Jordan 标准形 .....	82
§ 16	Euclid 空間 .....	90
§ 17	实数体与复数体,酉空間 .....	99
§ 18	正規变换 .....	103
§ 19	二次形式 Hermite 形式 .....	114
§ 20	多重綫性映射,張量积 .....	123
第 2 章	群, Boole 代数, 有限体 .....	132
§ 21	变换群的概念 .....	132
§ 22	群 .....	143
§ 23	Boole 代数 .....	151

§ 24	有限体 .....	156
第 3 章	有限群的表现論 .....	164
§ 25	表現空間与不变子空間,可約表現与既約表現 .....	164
§ 26	Schur 引理 .....	167
§ 27	完全可約表現 .....	170
§ 28	反步表現,張量积表現 .....	178
§ 29	群代数与正則表現 .....	179
§ 30	內自同构与伴隨表現 .....	186
§ 31	直交关系 .....	190
§ 32	特征标 .....	193
§ 33	群代数 $A(G)$ 的构造 .....	197
§ 34	群的直积的表現 .....	204
§ 35	誘導表現 .....	209
§ 36	特征标間的各种关系 .....	218
§ 37	群代数 $A(G)$ 的理想及幂等元 .....	228
§ 38	Young 的图形,台与盘 .....	235
§ 39	标准盘 .....	245
§ 40	标准盘的个数与对称群的既約表現的級数 .....	249
§ 41	对称群的既約表現的矩陣 .....	252
§ 42	Weyl 的相互律 .....	260
§ 43	一般綫性变换群的張量表現 .....	270
后 記	.....	280
附 录	有限旋轉群 .....	282

# 第1章 綫性代数

## § 1 向量及綫性运算

代数学与拓扑学在今天同是数学中龐大的基础部門之一。本书是“現代应用数学”中作为基础的代数学，以量子力学中所需用的“群表現論”为目标。对于作为数学而展开的代数学的各个部門自然不能广泛地都加以叙述。但是所謂群是什么，它的表現是什么，象这样一类問題，在引进时当然要写得使人容易理解。以下的叙述是在假定讀者已通曉物理数学初步（解析几何、微积分、简单微分方程的解法及其在力学上的应用等）的前提下进行的，此外不再有其他假定（希望讀者一面讀一面好好考虑其中相当丰富的例子）。

首先自向量开始，学过力学的讀者可能知道“有方向与大小的量”謂之向量。三維空間的向量  $\boldsymbol{x}$ ，采用空間坐标，可以用三个分量  $x_1, x_2, x_3$  来表示（图 1）。假定坐标系已确定，它就可写成

$$\boldsymbol{x} = (x_1, x_2, x_3), \quad (1.1)$$

或作为“列向量”写成

$$\boldsymbol{x} = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}. \quad (1.2)$$

（与此对应，(1.1)的右边叫做“行向量”）。

假定給定一个向量  $\boldsymbol{x}$  与一个数（数量） $\lambda$ ，那末“ $\boldsymbol{x}$  的  $\lambda$  倍” $\lambda\boldsymbol{x}$  这个向量就确定了。假定給定两个向量  $\boldsymbol{x}, \boldsymbol{y}$ ，那末它們的“和” $\boldsymbol{x} + \boldsymbol{y}$  这个向量也就确定了。它們的作法想讀者已知道（图 1.2）。如果用分量来表达，当  $\boldsymbol{x}$  用 (1.1)，而  $\boldsymbol{y}$  用

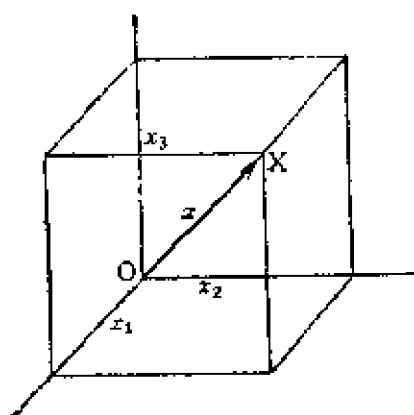


图 1.1

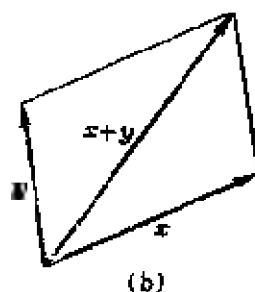
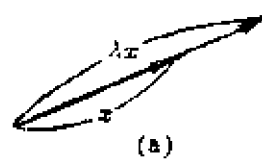


图 1.2

$$y = (y_1, y_2, y_3), \quad (1.3)$$

那末

$$\lambda x = (\lambda x_1, \lambda x_2, \lambda x_3), \quad (1.4)$$

$$x + y = (x_1 + y_1, x_2 + y_2, x_3 + y_3). \quad (1.5)$$

因而有下面的计算规则成立:

**交换律**

$$x + y = y + x, \quad (1.6)$$

**结合律**

$$(x + y) + z = x + (y + z). \quad (1.7)$$

在代数学中,这种“计算(也叫做运算,算法)规则”是值得重视的。对数学工作者来说,这不只是说说而已。例如由(1.6), (1.7)的交换律与结合律就能够得到如下事实的证明。

$$\begin{aligned} (x + y) + z &= (y + x) + z = y + (x + z) \\ &= y + (z + x) = \dots, \end{aligned}$$

这就是说,  $x, y, z$  三个向量有  $3! = 6$  种排列方法,而任意一种排列加上任何括弧所得的和都是相同的。有四个以上的向量时,同样的事实也成立。上述的  $x, y, z$  的和可省掉括弧而写成  $x + y + z$ 。一般有  $k$  个向量  $x_1, \dots, x_k$  时,它们的和用  $\sum_{i=1}^k x_i$  表示。总

之向量之間的加法能够象数之間的加法一样如常施行。这种事实成立的基础(即由它能够得到理論証明)或“公理”就是交換律, 結合律。

現在考虑加法的逆运算减法。假如考虑作为“基础”的零向量

$$\mathbf{0} = (0, 0, 0)$$

及(1.1)的逆向量

$$-\mathbf{x} = (-x_1, -x_2, -x_3),$$

那末对于任意  $\mathbf{x}$ ,

$$\mathbf{0} + \mathbf{x} = \mathbf{x} + \mathbf{0} = \mathbf{x},$$

$$\mathbf{x} + (-\mathbf{x}) = (-\mathbf{x}) + \mathbf{x} = \mathbf{0}.$$

因此, 如果把  $\mathbf{y} + (-\mathbf{x})$  写成  $\mathbf{y} - \mathbf{x}$ , 就有

$$(\mathbf{y} - \mathbf{x}) + \mathbf{x} = \mathbf{y}, \quad (\mathbf{y} + \mathbf{x}) - \mathbf{x} = \mathbf{y},$$

显然  $-\mathbf{x}$  是  $+\mathbf{x}$  的逆。总上所述, 得到

A. 向量之間加减法能够如常施行。

其中“如常”的意义也許有些模糊, 稍后将会明白。

作为 A 的基础之一的是交換律(1.6)。它在几何上已有証明, 由上面可知

$$\begin{aligned} \mathbf{x} + \mathbf{y} &= (x_1 + y_1, x_2 + y_2, x_3 + y_3) \\ &= (y_1 + x_1, y_2 + x_2, y_3 + x_3) \\ &= \mathbf{y} + \mathbf{x}. \end{aligned}$$

这第二边与第三边相等是由于数的加法服从交換律。同样, 由数的加法的結合律引出向量的結合律(1.7)。在数之間, 除加法的交換律、結合律之外, 乘法的交換律  $ab = ba$ , 結合律  $(ab)c = a(bc)$ , 加法与乘法之間的分配合律  $a(b+c) = ab+bc$  都成立。又对于任意数  $a$ ,  $1a = a$ 。由这些及(1.4), (1.5)可直接得到下面的 B。

B. 关于向量的数量倍, 下面的規則成立。

$$\lambda(\mathbf{x} + \mathbf{y}) = \lambda\mathbf{x} + \lambda\mathbf{y}, \quad (1.8)$$

$$(\lambda + \mu)x = \lambda x + \mu x, \quad (1.9)$$

$$(\lambda\mu)x = \lambda(\mu x), \quad (1.10)$$

$$1x = x. \quad (1.11)$$

这里  $\lambda, \mu$  是数量也就是数, 至于指的是那种数, 那并没有限制。但对于力学上所考虑的向量, 它当然是实数。实数有各种性质, 但是特別用在向量代数上的是它們之間加减乘除的四則运算能够如常施行。由于它的重要性, 特提出下面的 O。

O. 数量之間加减乘除运算能够如常施行 (这里“如常”的意义在稍后会清楚)。

向量之間的加减法及向量与数量的乘法叫做向量的“綫性运算”。因为减法是加  $(-1)$  倍, 所以把綫性运算說成“加法及数量倍”, 内容也不会改变。若对向量  $x_1, \dots, x_k$  重复施行綫性运算, 就得到象  $\sum_{i=1}^k \lambda_i x_i$  这样的向量。这  $\sum_{i=1}^k \lambda_i x_i$  叫做  $x_1, \dots, x_k$  的“1 次組合”, 或称为“綫性組合”。

以上說明了力学中所考虑的向量之間能够施行綫性运算, 并且揭示了 A, B, C 的成立。但同样的事实在数学的其他各个部門中也存在。例如就  $n$  阶綫性齐次常微分方程

$$\frac{d^n y}{dx^n} + p_1(x) \frac{d^{n-1} y}{dx^{n-1}} + \dots + p_n(x) y = 0 \quad (1.12)$$

的解来考虑, 这里系数  $p_i(x)$ ,  $i = 1, 2, \dots, n$ , 假定是  $x$  的解析函数, 那末这方程就有  $n$  个“独立”的基本解  $y_1^0(x), \dots, y_n^0(x)$ , 一般解  $y(x)$  能够表为它們的綫性組合  $\sum_{i=1}^n c_i y_i^0(x)$ , 这就是熟知的“迭加原理”。綫性組合中的系数(数量)  $c_i$  是复数。对于复数, 加减乘除能够如常施行, 即把复数看成数量, O 也成立。又假如  $y_1(x), y_2(x)$  是 (1.12) 的任意两个解, 那末  $y_1(x) + y_2(x)$ ,  $c y_1(x)$  ( $c$  是复数) 也是 (1.12) 的解。对于它們的綫性运算, 当然 A, B 成立。

## §2 关于现代代数学的方法

B. L. van der Waerden 有名的教科书《近世代数学》(Moderne Algebra) I, II 于 1930~1931 年初版发行, 此后又重版, 在最近的新版中, “近世” (Moderne) 两字已自标题中除去, 逕名为“代数学” (Algebra)。本书命名“代数学”是想同 van der Waerden 的代数学一样, 自由地应用现代代数学的方法。因为今天“现代代数学”就是“代数学”。关于其一般方法, 兹于此先进数言, 也许对读者会有好处。

作为它的方法的特征之一是“常采用集合论的记法”, 例如实数全体的集合用  $R$  表示, 复数全体的集合用  $C$  表示 (这种记法继续在本书中采用)。假如采用这种记法, 则“ $\lambda$  是实数”这个事实就用“ $\lambda \in R$ ” (或“ $R \ni \lambda$ ”) 表示。又“实数是复数” (的一种) 这一事实用“ $R \subset C$ ” (或“ $C \supset R$ ”) 表示。一般, “ $x \in M$ ” (或“ $M \ni x$ ”) 就是“ $x$  是  $M$  中之元 (或元素)”, 换言之, 即“ $x$  属于集合  $M$ ”, “ $M_1 \supset M_2$ ” (或“ $M_2 \subset M_1$ ”) 就是“集合  $M_2$  是  $M_1$  的子集合”, 亦即“ $M_2$  中之元都是  $M_1$  中之元”。集合  $M_1, M_2, \dots, M_k$  的和集或并集 (即属于  $M_1, M_2, \dots, M_k$  中任意一个的元全体所成的集合) 用  $M_1 \cup M_2 \cup \dots \cup M_k$  或  $\bigcup_{i=1}^n M_i$  表示。 $M_1, M_2, \dots, M_k$  的通集或交集 (即同时属于所有  $M_1, M_2, \dots, M_k$  的元全体的集合) 用  $M_1 \cap M_2 \cap \dots \cap M_k$  或  $\bigcap_{i=1}^k M_i$  表示。属于  $M_1$  而不属于  $M_2$  的元全体的集合用  $M_1 - M_2$  表示。空集 (即不包含元的集合) 用  $\emptyset$  表示 (例如  $M \cup M = M \cap M = M, M - M = \emptyset$ )。

第二个特征是“算法与算法规则的重视”, 关于这方面, 在前面已提及, 今后这样的例子也到处可以看到, 不再重述。

第三个特征是“抽象化, 公理化的方法”。为防止消极的理解,



在这里特强调它的积极意义。数学原来是抽象的学问。1, 2, 3, ... 这些自然数是从1个人, 2只鳥, 3个苹果, ... 等抽象得到的, 正因为它是被抽象出来的概念, 所以应用广泛。

在前面已看到对于力学中所使用的向量, 对于齐次綫性常微分方程的解,  $A, B, C$  都成立。于是, 仅只从  $A, B, C$  依邏輯方法演繹而得的理論, 在任何場合—— $A, B, C$  成立的所有場合——都能够应用。这时对所考虑的形象, 只想着是力学中的向量就可以了。这样, 通过直观考察作为仅只由  $A, B, C$  推証的結果 (在初等几何学中, 以图形为背景所考虑的証明与通过公理、定理推証的吻合), 在微分方程論以及其他各分支中都有运用的可能性。因此不得不把  $A, B, C$  的内容用含义清晰的公理来叙述。这就是“抽象化, 公理化方法”的說明。

最后要注意在抽象代数学中文字不一定表示数 (不要拘泥于“代数”这个字面), 文字可以表示向量、集合及其他各种东西。

### §3 作为代数系的向量空間

由上面的說明, 首先使 §1,  $A$  的内容清楚了。

在  $A$  是說向量之間“加減法能够如常施行”。一般所謂“在某集  $S$  中加減法能够如常施行”, 其意义由下面五个公理来定义。

A1.  $S$  是非空集, 对于  $x, y \in S$ ,  $x, y$  的“和”  $x+y \in S$  是唯一确定的 (使  $x, y$  对应于  $x+y$  的算法, 叫做“加法”)。

A2.  $x+y=y+x$  (交換律)。

A3.  $(x+y)+z=x+(y+z)$  (結合律)。

A4. 对于  $S$  中任意元  $x$ ,  $S$  中有 1 个适合  $x+0=0+x=x$  这样的元  $0$  存在, 它叫做零元。

A5. 对于  $x \in S$ , 有适合  $(-x)+x=x+(-x)=0$  这样的“元  $(-x) \in S$  存在”。

这事实与常識上所考虑的“在  $S$  中加减法能够如常施行”有同样意义。这由 § 1, A 前面的說明大致可以明白。

一般, 满足 A1~5 的集叫做**加群**。假如引用这概念, § 1, A 就是說“向量的集形成加群”。

**例 1** 在加群  $S$  中,  $x+y=x+z \Rightarrow y=z$ 。

[解] 两边自左加  $(-x)$ , 得

$$(-x) + (x+y) = (-x) + (x+z).$$

由 A3,  $((-x) + x) + y = ((-x) + x) + z,$

由 A5,  $0 + y = 0 + z,$

由 A4,  $y = z.$

**例 2** 在加群  $S$  中,

$$x+y=x \Rightarrow y=0, \quad x+y=0 \Rightarrow y=-x.$$

(因此, A4 中的 0 及 A5 中的  $-x$  是唯一确定的。)

[解] 由例 1 即得。

**例 3**  $-(-x)=x$  (命  $-x=y$ , 再用  $-y$  的唯一性)。

把加群的概念更进一步抽象化, 就得到下面可换群的概念。

A°1. 假定  $S$  是非空集合, 对于  $x, y \in S$ , 給定了与  $S$  中元  $x \circ y$  唯一对应的算法:

A°2.  $x \circ y = y \circ x$  (交换律)。

A°3.  $(x \circ y) \circ z = x \circ (y \circ z)$  (結合律)。

A°4. 对于  $S$  中任意元  $x$ ,  $S$  中存在 1 个满足  $x \circ e = e \circ x = x$  这样的元  $e$ 。

A°5. 对于  $x \in S$ , 存在满足  $x' \circ x = x \circ x' = e$  这样的元  $x' \in S$ 。

满足 A°1~5 这样的集  $S$  叫做关于算法  $\circ$  的**可换群**。A°4 中的  $e$  叫做可换群  $S$  的**单位元**, A°5 中的  $x'$  叫做  $x$  的**逆元**。

加群就是关于加法的可换群。在加群中单位元写成 0,  $x$  的逆元写成  $-x$ 。

例如: 在实数之間加减法当然能够如常施行, 所以  $R$  成为加

群。在从  $R$  除去 0 后所成的集  $R^* = R - \{0\}$  ( $\{0\}$  表示只由 0 形成的集) 中, 因为乘除法“能够如常施行”, 所以  $R^*$  关于乘法做成可换群。它的单位元是 1,  $x$  的逆元是  $x$  的倒数  $x^{-1} = \frac{1}{x}$ 。在  $R$  中, 乘法不仅对  $R^*$  中元可行, 即使对 0 也有定义, 并且在加法与乘法之间成立着

$$\text{分配律} \quad x(y+z) = xy + xz.$$

“通常的四则运算”就是根据这些规则来施行的。因此“在某集  $K$  中加减乘除能够如常施行”由下面 O1~4 来定义。

O1.  $K$  是至少含有两个元的集合。对于  $x, y \in K$ , 存在着分别唯一地对应于“和”  $x+y$  的“加法”及对应于“积”  $xy$  的“乘法”。

O2.  $K$  成为加群(它的单位元用 0 表示)。

O3.  $K - \{0\} = K^*$  关于乘法成为可换群(它的单位元用 1 表示)。

O4. 分配律(3.1)成立。

满足 O1~4 的集叫做体。由于  $R, C$  成为体, 所以分别叫做实数体与复数体。第 4 页 O 换言之就是“数量的集成为体”。

**例 4** 在体  $K$  中, 必有  $0 \cdot x = 0, (-x)y = x(-y) = -xy, (-x)(-y) = xy$ 。

[解] 由 0 的定义,  $0+y=y$ , 由分配律,  $(0-y)x=0x+yx=yx$ 。由于  $K$  是加群, 所以根据 0 的唯一性(例 2),  $0x=0$ 。又因为  $0=0y=(x+(-x))y=xy+(-x)y$ , 由  $-xy$  的唯一性,  $-xy=(-x)y$ 。同样,  $-xy=x(-y)$ 。用例 3, 即得  $(-x)(-y)=xy$ 。

**例 5** 在体  $K$  中, 如果  $x \neq 0$ , 则  $xy=0 \Rightarrow y=0$ 。

[解] 因为  $x \neq 0$ , 所以  $x^{-1}$  存在。用  $x^{-1}$  左乘  $xy=0$  的两边, 即得。

上面的加群, 可换群, 体, 都能够象下面那样来定义, 即

(i) 有某集合, 在这集合中定义了某种算法。

(ii) 这些算法满足所给定的几个法则。

一般, 把“在它的元之间能够进行满足某法则的算法的集合”

叫做以这算法做“基本算法”的代数系。加群,可换群,体,都是代数系的特例。现代代数学,用一句话来说,那就是“代数系的理论”。

体  $K$  给定时,“ $K$  上向量空间” $V$  定义为满足下面 A, B1~5 的代数系。

A.  $V$  成为加群。

B1. 当  $x \in V$ ,  $\lambda \in K$  给定时,“ $x$  的  $\lambda$  倍” $\lambda x$  也在  $V$  中,而且是唯一确定的。

B2. 对于  $x, y \in V$ ,  $\lambda \in K$ , 有  $\lambda(x+y) = \lambda x + \lambda y$ .

B3. 当  $x \in V$ ,  $\lambda, \mu \in K$ , 有  $(\lambda + \mu)x = \lambda x + \mu x$ .

B4. 当  $x \in V$ ,  $\lambda, \mu \in K$ , 有  $(\lambda\mu)x = \lambda(\mu x)$ .

B5.  $1 \cdot x = x$ .

**注意** 向量空间也叫做线性空间或线性流形。又“ $K$  上向量空间”也叫做  $K$  加群。 $K$  叫做  $K$  上向量空间的基础体。

**例 6** 在体  $K$  上向量空间中,

$$0x = 0, (-1)x = -x, (-\lambda)x = -\lambda x,$$

$$\lambda x = 0, \lambda \neq 0 \Leftrightarrow x = 0.$$

[解] 与例 4, 5 同样推得。

§1 所说“在力学中使用的向量”是  $R$  上向量空间中元。线性微分方程的解是  $C$  上向量空间中元 (也许甚至还有人认为把微分方程解的集合叫做“向量空间”是不适当的,但由 §2 所述,这样命名不但没有妨碍,而且反而便利)。

在本书中讨论的所谓“线性代数”无非是“体  $K$  上向量空间”这个代数系的理论。因此,本节的公理 A, B, C 是全部的基础。但是不习惯这样考虑的读者只要把在 §1 中所示的大体了解为公理也就可以了。

**例 7** 体  $K$  自身可以看做  $K$  上向量空间。

[解] 例如把  $x+y$  ( $x \in K, y \in K$ ),  $\lambda x$  ( $\lambda \in K, x \in K$ ) 分别当作在  $K$  中定义加法及乘法,那末公理 A1~5, B1~5 能够满足。

**例 8** 假定  $n$  是給定的自然数, 由体  $K$  中  $n$  个元所作的行向量  $(\xi_1, \xi_2, \dots, \xi_n)$  (或叫做  $K$  上  $n$ -行向量) 用  $x$  表示:  $x = (\xi_1, \xi_2, \dots, \xi_n)$ . 假設这样  $x$  全体的集合是

$${}^nK = \{x; x = (\xi_1, \xi_2, \dots, \xi_n), \xi_i \in K\}.$$

(一般  $\{x; \dots\}$  是表示“具有……性质的  $x$  全体的集合”。这記法今后常采用。) 对于  $x = (\xi_1, \xi_2, \dots, \xi_n) \in {}^nK, y = (\eta_1, \eta_2, \dots, \eta_n) \in {}^nK, \lambda \in K$ , 如果定义  $x + y = (\xi_1 + \eta_1, \xi_2 + \eta_2, \dots, \xi_n + \eta_n), \lambda x = (\lambda \xi_1, \lambda \xi_2, \dots, \lambda \xi_n)$ , 那末  ${}^nK$  成为  $K$  上向量空間。命  ${}_1e = (1, 0, \dots, 0), {}_2e = (0, 1, 0, \dots, 0), \dots, {}_ne = (0, \dots, 0, 1)$ , 于是  $x = (\xi_1, \dots, \xi_n) = \xi_1 \cdot {}_1e + \dots + \xi_n \cdot {}_ne$ . 同样, “ $K$  上  $n$  列向量 (其意义自明) 的集合  $K^n$  也是  $K$  上向量空間。

**例 9** 假定由体  $K$  中无穷多个元所成的集合是

$${}^\infty K = \{x; x = (\xi_1, \xi_2, \dots), \xi_i \in K\}.$$

对于  $x = (\xi_1, \xi_2, \dots), y = (\eta_1, \eta_2, \dots) \in {}^\infty K, \lambda \in K$ , 如果定义

$$x = y \Leftrightarrow \text{对于所有的 } n, \xi_n = \eta_n,$$

$$x + y = (\xi_1 + \eta_1, \xi_2 + \eta_2, \dots), \lambda x = (\lambda \xi_1, \lambda \xi_2, \dots),$$

那末  ${}^\infty K$  成为  $K$  上向量空間。

**例 10** 假定  $a, b \in \mathbf{R}$ , 那末集合  $\{x; a \leq x \leq b\}$  叫做閉区間, 用  $[a, b]$  表示。又  $\{x; a < x < b\}$  叫做开区間, 用  $(a, b)$  表示。开区間、閉区間和下面的各集合总称为区間。

$$(a, b] = \{x; a < x \leq b\}, [a, b) = \{x; a \leq x < b\},$$

$$(-\infty, b] = \{x; x \leq b\}, [a, +\infty) = \{x; a \leq x\},$$

$$(-\infty, b) = \{x; x < b\}, (a, +\infty) = \{x; a < x\}, (-\infty, \infty) = \mathbf{R}.$$

定义于  $[a, b]$  取实数值的函数全体的集合表为

$$\mathfrak{F}([a, b], \mathbf{R}) = \{f; x \in [a, b], f(x) \in \mathbf{R}\}.$$

(当  $[a, b]$  給定, 不致引起誤解时, 也常单用  $\mathfrak{F}$  表示。) 对于  $f, g$ , 如果定义

$$f = g \Leftrightarrow \text{对于所有 } x \in [a, b], f(x) = g(x),$$

$$\text{对于所有 } x, (f + g)(x) = f(x) + g(x), (\lambda f)(x) = \lambda f(x), (\lambda \in \mathbf{R}),$$

显然  $\mathfrak{F}$  成为  $\mathbf{R}$  上向量空間。

在  $\mathfrak{F}$  的子集中, 假定所有連續函数的集合是  $\mathfrak{C}^0([a, b], \mathbf{R})$ , 根据上面的和,  $\lambda$  倍的定义, 它也成为  $\mathbf{R}$  上向量空間。更在  $[a, b]$  中, 假定  $n$  阶連續可微函数全体的集合是  $\mathfrak{C}^n([a, b], \mathbf{R})$ , 无限阶連續可微函数全体的集合是  $\mathfrak{C}^\infty([a, b], \mathbf{R})$ , 它們根据同样定义, 也成为  $\mathbf{R}$  上向量空間。

在  $\mathfrak{C}^0$  的子集中, 假定在  $[a, b]$  內解析 (即对于  $[a, b]$  中各点  $x_0$ ,  $f(x)$  在  $x_0$  邻域的值可用  $x-x_0$  的幂級数来表示) 函数全体的集合写成  $\mathfrak{A}([a, b], \mathbf{R})$ , 則它根据同样定义, 也成为  $\mathbf{R}$  上向量空間。

取区間  $\Delta$  来代替  $[a, b]$ , 考虑  $\mathfrak{F}(\Delta, \mathbf{R})$ ,  $\mathfrak{C}^0(\Delta, \mathbf{R})$ ,  $\mathfrak{C}^n(\Delta, \mathbf{R})$ ,  $\mathfrak{C}^\infty(\Delta, \mathbf{R})$ ,  $\mathfrak{A}(\Delta, \mathbf{R})$ , 它們的定义是明显的。它們也能够成为  $\mathbf{R}$  上向量空間。对于任意区間  $\Delta$ , 显然  $\mathfrak{F} \supset \mathfrak{C}^0 \supset \mathfrak{C}^1 \supset \mathfrak{C}^2 \supset \dots \supset \mathfrak{C}^\infty \supset \mathfrak{A}$ 。

又对于定义在复数平面区域  $D$  中的复值函数, 同样定义  $\mathfrak{F}(D, \mathbf{C})$ ,  $\mathfrak{A}(D, \mathbf{C})$ , 它們都成为  $\mathbf{C}$  上向量空間,  $\mathfrak{F} \supset \mathfrak{A}$ 。

由以上所定义的这些函数, 形成的各种向量空間, 总称为函数空間。

## § 4 子空間, 生成元, 直和分解

以后我們約定, 体  $K$  上向量空間用  $V$  表示,  $K$  之元 (叫做数量) 用希腊字母  $\alpha, \beta, \dots$  表示,  $V$  之元 (叫做向量) 用  $x, y, z, \dots$  (必要时附加添数) 表示。  $K$  的加群的单位元  $0$  与  $V$  的  $0$  用同一的記号表示。假如注意前后关系, 当不致引起混淆。

向量空間的基本算法是加法与“数量倍”。这两种算法合称为綫性运算 (也叫做 1 次运算, 1 次算法等。“綫性”与“1 次”, “运算”与“算法”是同义的)。关于向量空間  $V$  的子集  $M_1, M_2$ , 有下面的記法

$$M_1 + M_2 = \{x_1 + x_2; x_1 \in M_1, x_2 \in M_2\}, \quad (4.1)$$

$$\lambda M_1 = \{\lambda x_1; x_1 \in M_1\}. \quad (4.2)$$

((4.1) 的右边表示  $M_1$  中元  $x_1$  与  $M_2$  中元  $x_2$  的和  $x_1 + x_2$  全体的集合, (4.2) 的右边表示  $M_1$  中元  $x_1$  的  $\lambda$  倍  $\lambda x_1$  全体的集合。这样的記法, 今后常常采用, 参照 § 3, 例 8)。

$$\begin{aligned} \text{例 1} \quad V + V &= V, \quad \lambda V = V, \\ \{0\} + \{0\} &= \{0\}, \quad \lambda \{0\} = \{0\}. \end{aligned}$$

$V$  的子集  $W (\neq \emptyset)$  假如满足下面两个条件:

$$(a) \quad W' + W' \subset W,$$

(b) 对于任意  $\lambda \in K$ ,  $\lambda W \subset W$ ,

那末我們就說  $W$  “关于綫性运算是閉的”。这时  $W$  滿足 §3, A1, B1. 因为对于  $V$ , A2, 3, B2~5 滿足, 所以对于它的子集  $W$ , 这些条件也成立。再假如  $x \in W$  (因为  $W \neq \emptyset$ , 所以这样的  $x$  是存在的), 那末  $0x = 0$ ,  $(-1)x = -x$  (§3, 例6)。所以由 (b),  $0 \in W$ ,  $x \in W \Rightarrow -x \in W$ . 即 A4, A5 也成立, 于是  $W$  成为向量空間。因此滿足 (a), (b) 的  $W \subset V$  叫做  $V$  的**子空間** (一般, 对于某代数系  $S, T \subset S$ , 假如在上面同样的意义下, “关于  $S$  的基本算法是閉的”, 那末  $T$  也与  $S$  同样成为代数系。这时  $T$  叫做  $S$  的**子系**)。

**例2**  $V$  及  $\{0\}$  成为  $V$  的子空間 (参照例1)。又假如  $W$  是任意子空間, 那末  $V \supset W \supset \{0\}$ .

**例3** 假如 (a) 成立, 那末  $W + W = W$ . 又当 (b) 成立时, 假如  $\lambda \neq 0$ , 那末  $\lambda W = W$ . (由 A4, B4, 5, C3.) ①

今后暂时固定  $V$ , 凡子空間是指  $V$  的子空間, 子空間全体的集合用  $\mathfrak{B}$  表示。

**命题 ①**  $\mathfrak{B} \ni W_1, W_2 \Rightarrow W_1 \cap W_2 \in \mathfrak{B}$ .

一般 ②,  $\{W_\alpha\} \subset \mathfrak{B} \Rightarrow \bigcap_\alpha W_\alpha \in \mathfrak{B}$ .

**証明**  $W_\alpha \in \mathfrak{B}$ , 命  $W = \bigcap_\alpha W_\alpha$ , 对于  $W$ , 証明 (a), (b) 成立即可。

假定  $x, y \in W$ , 那末对于所有的添数  $\alpha$ ,  $x, y \in W_\alpha$ . 因为  $W_\alpha \in \mathfrak{B}$ , 所以  $x + y \in W_\alpha$ ,  $\lambda x \in W_\alpha$ . 因为这对于所有的  $\alpha$  成立, 所以  $x + y \in W$ ,  $\lambda x \in W$ .

① 由 A4, 对于  $x \in W$ ,  $x = 0 + x \in W + W$  即  $W \subset W + W$ , 所以  $W = W + W$ . 又由 B5,  $x = 1 \cdot x$ , 由 C3,  $1 = \lambda \cdot \frac{1}{\lambda}$ , 因此  $x = 1 \cdot x = \left(\lambda \cdot \frac{1}{\lambda}\right) x = \lambda \left(\frac{1}{\lambda} x\right)$  (由 B4). 但  $\frac{1}{\lambda} x \in \frac{1}{\lambda} W \subset W$ , 于是  $x \in \lambda W$  即  $W \subset \lambda W$ , 所以  $\lambda W = W$ . ——譯者注

② 以下, 把定理中意义較輕的叫做“命题”。定理是这样叙述的, 只讀它就可以理解。但“命题”中有时对有关記法, 不加說明。

③  $\{W_\alpha\}$  是有添数  $\alpha$  (有限个或无限个) 的  $W_\alpha$  的集合。

**命題 2** 假定  $M$  是  $V$  的任意子集, 那就存在唯一含  $M$  的“最小”子空間  $W$ , 即唯一存在  $W$  满足:

(i)  $W \in \mathfrak{B}$ , (ii)  $W \supset M$ , (iii)  $W_1 \in \mathfrak{B}, W_1 \supset M \Rightarrow W_1 \supset W$ .

**証明** 假定含  $M$  的子空間全体的集合是  $\{W_\alpha\}$ ,  $\bigcap_{\alpha} W_\alpha = W$ , 由命題 1, (i) 成立。(ii) 是明显的。又假如  $W_1 \in \mathfrak{B}, W_1 \supset M$ , 因为  $W_1$  是含  $M$  的子空間, 所以可以看成是 1 个  $W_\alpha$ , 因此 (iii) 成立。

再假定 (i')  $W' \in \mathfrak{B}$ , (ii')  $W' \supset M$ , (iii')  $W'_1 \in \mathfrak{B}, W'_1 \supset M \Rightarrow W'_1 \supset W$ , 由 (i'), (ii'), (iii) (在 (iii) 考虑  $W_1 - W'$ ),  $W' \supset W$ . 又由 (i), (ii), (iii'),  $W \supset W'$ , 因此  $W = W'$ . (証毕)

在命題 2 中所确定的  $W$  叫做由  $M$  生成的子空間, 用  $[M]$  表示。当  $M = M_1 \cup M_2 \cup \cdots \cup M_k$  时,  $[M]$  写成  $[M_1, M_2, \cdots, M_k]$ . 当  $M$  是由有限个元  $x_1, x_2, \cdots, x_k$  构成时 (即  $M = \{x_1, x_2, \cdots, x_k\}$  时),  $[M]$  写成  $[x_1, x_2, \cdots, x_k]$ . 又这时  $x_1, x_2, \cdots, x_k$  叫做  $[x_1, x_2, \cdots, x_k]$  的生成元。

**例 4**  $M_1 \supset M_2 \Rightarrow [M_1] \supset [M_2]$ ;  $W \in \mathfrak{B} \Leftrightarrow W = [W]$ ;  $[[M]] = [M]$ .

**命題 3**  $W_1, W_2 \in \mathfrak{B} \Rightarrow [W_1, W_2] = W_1 + W_2$ .

**証明** 假定  $W = [W_1, W_2]$ ,  $W' = W_1 + W_2 = \{x_1 + x_2; x_1 \in W_1, x_2 \in W_2\}$ , 因此只要証明 (i)  $W \supset W'$ , (ii)  $W' \supset W$  即可。

(i) 因为  $W \in \mathfrak{B}, W_1, W_2 \subset W, x_1 \in W_1, x_2 \in W_2$ , 根据子空間的条件 (a),  $x_1 + x_2 \in W$ , 所以  $W' \subset W$ .

(ii) 因为  $0 \in W_2$ , 所以对于任意  $x_1 \in W_1, x_1 = x_1 + 0 \in W'$ , 于是  $W_1 \subset W'$ . 同样  $W_2 \subset W'$ . 因此, 假如能够証明  $W' \in \mathfrak{B}$ , 由命題 2 (iii), 即得  $W' \supset W$  ①.

---

① 这时  $W = [W_1, W_2]$ ,  $M = W_1 \cup W_2$ . 因为  $W_1 \subset W', W_2 \subset W'$  所以  $W' \supset W_1 \cup W_2$  即  $W' \supset M$ . 因此, 假如  $W' \in \mathfrak{B}$  成立, 由命題 2 的 (iii) 即得  $W' \supset W$ .  
——譯者注



$W' \in \mathfrak{B}$  的证明: 假定  $x_1 + x_2, x'_1 + x'_2 \in W'$  ( $x_i, x'_i \in W_i, i = 1, 2$ ), 那末  $(x_1 + x_2) + (x'_1 + x'_2) = (x_1 + x'_1) + (x_2 + x'_2) \in W'$ . 又  $\lambda(x_1 + x_2) = \lambda x_1 + \lambda x_2 \in W'$ , 即  $W'$  满足 (a), (b).

**系 1**  $W_1, W_2, \dots, W_k \in \mathfrak{B} \Rightarrow [W_1, W_2, \dots, W_k] = W_1 + W_2 + \dots + W_k$ .

**系 2**  $[x_1, x_2, \dots, x_k] = \{\lambda_1 x_1 + \lambda_2 x_2 + \dots + \lambda_k x_k; \lambda_i \in K\}$  ①.

**例 5**  ${}^n K = [{}_1 e, {}_2 e, \dots, {}_n e]$  (§ 3 例 8 的记法)。

又假如

$$e_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \quad e_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \quad \dots, \quad e_n = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix},$$

那末,

$$K^n = [e_1, e_2, \dots, e_n].$$

$W_1, W_2, \dots, W_k \in \mathfrak{B}$  时,  $W = [W_1, \dots, W_k] = W_1 + W_2 + \dots + W_k (\in \mathfrak{B})$  叫做  $W_1, W_2, \dots, W_k$  的**和或和空间**, 写成  $W = \sum_{i=1}^k W_i$ . 关于它的子空间之间的“加法”, 显然交换律与结合律都成立。 $\{0\} \in \mathfrak{B}$  是它的“加法”的单位元。

假定  $W = \sum_{i=1}^k W_i$ , 那末  $W$  中任意元  $w$  可以表成  $\sum_{i=1}^k w_i$  的形状, 但是这表示不一定是唯一的。如果这表示是唯一的, 那末  $W$  叫做  $W_1, W_2, \dots, W_k$  的**直和**, 写成  $W = W_1 \oplus W_2 \oplus \dots \oplus W_k$  或  $\sum_{i=1}^k \oplus W_i$ , 这一表式称为  $W$  的**直和分解**,  $W_i$  叫做这分解的**直和因子**。假如  $\{0\} = W_0$ , 显然  $W = \sum_{i=1}^k \oplus W_i \Rightarrow W = \sum_{i=0}^k \oplus W_i$ . 又假如在  $W_1, W_2,$

① 因为  $[x_i]$  是含  $x_i$  的最小子空间, 显然它是由  $\lambda x_i, \lambda \in K$  构成的, 因此  $[x_i] = \{\lambda x_i, \lambda \in K\}$ , 于是  $[x_1, x_2, \dots, x_k] = [[x_1], [x_2], \dots, [x_k]] = [x_1] + [x_2] + \dots + [x_k] = \{\lambda_1 x_1 + \lambda_2 x_2 + \dots + \lambda_k x_k, \lambda_i \in K\}$ . ——译者注

$\cdots, W_k$  中有等于  $W_0$  的, 譬如  $W_1 = W_0$ , 那末  $W = \sum_{i=1}^k \oplus W_i \Rightarrow W = \sum_{i=2}^k \oplus W_i$ . 这样, 因为  $\{0\}$  作为直和因子是无关紧要 (irrelevant) 的, 所以今后不特别声明,  $\{0\}$  不考虑作为直和因子。

**例 6**  ${}^n K = [{}_1 e] \oplus \cdots \oplus [{}_n e], K^n = [e_1] \oplus \cdots \oplus [e_n]$ .

直和分解

$$W = W_1 \oplus \cdots \oplus W_k \quad (4.3)$$

給出时, 任意元  $x \in W$  可以唯一地写成

$$x = x_1 + \cdots + x_k, \quad x_i \in W_i. \quad (4.4)$$

这时  $x_i$  叫做  $x$  的  $W_i$  分量。設  $W$  中元  $y$  的  $W_i$  分量是  $y_i$ , 那末

$$y = y_1 + \cdots + y_k, \quad (4.5)$$

由 (4.4), (4.5) 得

$$x + y = (x_1 + y_1) + \cdots + (x_k + y_k), \quad (4.6)$$

$$\lambda x = \lambda x_1 + \cdots + \lambda x_k. \quad (4.7)$$

因为  $x_i + y_i \in W_i, \lambda x_i \in W_i$ , 所以 (4.6), (4.7) 給出  $x + y, \lambda x$  各  $W_i$  分量的分解。

直和概念, 对于其他代数系也可定义 (代数系的基本算法是乘法的形状时, 又命名为“直积”)。在现代代数学一般观点下, 这一概念颇为重要, 所以下面另述一种說法。

一般,  $k$  个集合  $M_1, \cdots, M_k$  ( $k$  为自然数) 的直积  $M = M_1 \times \cdots \times M_k$  定义为由这  $k$  个集合中元形成的元組 ( $k$  重) 的集合

$$\{(x_1, \cdots, x_k); x_i \in M_i\}.$$

两个組  $(x_1, \cdots, x_k)$  与  $(x'_1, \cdots, x'_k)$  当  $x_1 = x'_1, \cdots, x_k = x'_k$  时且限于这时定义为相等。

**例 7** 假定  $M_1, \cdots, M_k$  都是有限集合, 它們分別有  $m_1, \cdots, m_k$  个元, 那末  $M_1 \times \cdots \times M_k$  是由  $m_1 \cdots m_k$  个元所构成。

于是, 当  $k$  个向量空間  $V_1, \cdots, V_k$  給定时, 在它們的直积  $V$

中,元組之間可定义如下的綫性运算:

$$(x_1, \dots, x_k) + (y_1, \dots, y_k) = (x_1 + y_1, \dots, x_k + y_k),$$

$$\lambda(x_1, \dots, x_k) = (\lambda x_1, \dots, \lambda x_k).$$

这样,  $V$  成为向量空間是很明显的(参照 §1)。这时  $V$  叫做  $V_1, \dots, V_k$  的直和,写成  $V_1 \oplus \dots \oplus V_k$ 。

上面直和的概念有了两种定义,說明它們在实质上一致是必要的。为此应先叙述在一般現代代数学中重要的同构的概念。

假定有两个向量空間  $V$  及  $V'$ ,  $f$  是自  $V$  到  $V'$  的一对一的映射(关于映射的詳述,参照后面的 §6),即对于  $x \in V$ ,  $x$  在映射  $f$  下的象  $f(x) \in V'$  唯一确定,这时 (1)  $f(x_1) = f(x_2) \Rightarrow x_1 = x_2$  (这时叫  $f$  是一对一的); (2)  $\{f(x); x \in V\} = V'$  (这时叫  $f$  是把  $V$  映成  $V'$  的映射)成立。并且

$$f(x+y) = f(x) + f(y),$$

$$f(ax) = \lambda f(x).$$

(这时映射  $f$  叫做保存綫性运算),那末  $f$  叫做自  $V$  到  $V'$  的同构映射。这样的同构映射存在时  $V$  与  $V'$  叫做同构,記为  $V \cong V'$  (在一般的代数系中,对于同种的代数系  $S, S'$ ,假如有自  $S$  到  $S'$  上的一对一的保存基本算法的映射,那末  $S, S'$  叫做同构,这样的映射叫做同构映射)。同构关系显然是等价关系,即

**反射律**  $V \cong V$ ,

**对称律**  $V \cong V' \Rightarrow V' \cong V$ ,

**推移律**  $V \cong V', V' \cong V'' \Rightarrow V \cong V''$ 。

(一般满足反射、对称、推移三律的关系叫做等价关系。)同构的代数系也称为“是具有同样的构造”。

回到前面,来証明上面直和的两种定义实质上是一致的。首先,为了区别它們,假定根据第一个定义,  $W_1, \dots, W_k$  的直和象前面一样用  $W = \sum_{i=1}^k \oplus W_i$  表示,根据第二定义,  $W_1, \dots, W_k$  的直

和用  $\dot{W} = \sum_{i=1}^k \dot{\oplus} W_i$  表示。我們將証明  $W \cong \dot{W}$ 。为此,对于

$$x = x_1 + \cdots + x_k \in W,$$

使与

$$(x_1, \cdots, x_k) \in \dot{W}$$

对应即可。即假定  $f(x) = (x_1, \cdots, x_k) \in \dot{W}$ 。容易知道这  $f$  是自  $W$  到  $\dot{W}$  的同构映射。因此以后  $\Sigma \dot{\oplus}$  这样的記法不再采用,但是  $\Sigma \dot{\oplus} W_i$  的构造由  $W_i$  的构造确定,而且在  $W = \Sigma \dot{\oplus} W_i$  时,  $W_i$  一般是比  $W$  “小”的向量空間。于是假如  $W$  能够直和分解,那末  $W$  的构造可以用比  $W$  小的空間的构造来确定。这事实有利于問題的簡化,今后将一再引用。

$V$  的任意子空間  $W_1, \cdots, W_k$  的和空間总是存在的,但它一般不是直和(例:設  $V \neq \{0\}$ , 那末  $V = V + V \neq V \dot{\oplus} V$ )。首先,因为不考虑把  $\{0\}$  作为直和因子,决定用  $\mathfrak{B}^*$  来表示  $\mathfrak{B} - \{0\}$ 。对于  $W_1, \cdots, W_k \in \mathfrak{B}^*$  ( $k \geq 2$ ), 如果  $W_1 + \cdots + W_k = W_1 \dot{\oplus} \cdots \dot{\oplus} W_k$ , 則称  $W_1, \cdots, W_k$  无关(仅只一个  $W_1 \in \mathfrak{B}^*$  总是叫做无关)。其次我們来証明下面一个关于判定  $\mathfrak{B}^*$  的空間无关性的定理来結束本节,为了自然地引进定理的証明,先举它的一个特例,即下面的引理。

**引理 1** 假定  $W_1, W_2 \in \mathfrak{B}^*$ ,  $W_1 \cap W_2 = \{0\}$ , 那末  $W_1, W_2$  无关。

**証明** 对偶地証明“假定  $W_1, W_2 \in \mathfrak{B}^*$  而  $W_1, W_2$  相关,那末  $W_1 \cap W_2 \neq \{0\}$ ”。

若  $W_1, W_2$  相关,那就有  $x_1 + x_2 = x'_1 + x'_2$ ,  $x_i, x'_i \in W_i$ ,  $i = 1, 2$ , 并且  $x_i \neq x'_i$ 。将上式移項得  $x_1 - x'_1 = x'_2 - x_2$ , 它的左边  $\in W_1$  而右边  $\in W_2$ , 所以  $\in W_1 \cap W_2$ , 但这元不是 0。

**定理 1** 向量空間  $V$  中异于  $\{0\}$  的子空間  $W_1, \cdots, W_k$  ( $k$  是自然数  $\geq 2$ ) 成为无关,下面的 (i) ~ (iv) 都是必要充分条件。

(i)  $x_1 + \cdots + x_k = 0, x_i \in W_i \Rightarrow x_i = 0, i = 1, \cdots, k$ 。

(ii)  $W_1, \dots, W_{k-1}$  无关,  $(W_1 + \dots + W_{k-1}) \cap W_k = \{0\}$ .

(iii)  $(W_1 + \dots + W_{i-1} + W_{i+1} + \dots + W_k) \cap W_i = \{0\}$ ,  $i = 1, \dots, k$ .

(iv)  $W_1 \cap W_2 = \{0\}$ ,  $(W_1 + W_2) \cap W_3 = \{0\}$ ,  $\dots$ ,  $(W_1 + \dots + W_{k-1}) \cap W_k = \{0\}$ .

**証明** 把  $W_1, \dots, W_k$  无关这个条件作为(0), 依这样的順序  
 $(0) \Rightarrow (i) \Rightarrow (ii) \Rightarrow (0)$ ,  $(0) \Rightarrow (iii) \Rightarrow (i)$ ,  $(0) \Rightarrow (iv) \Rightarrow (i)$  来証明。  
 (0) 詳細說就是

$$W = \sum_{i=1}^k W_i = \sum_{i=1}^k \oplus W_i,$$

这意味着  $x \in W$  象 (4.4) 那样的分解是唯一的。但要注意它与  $W_1, \dots, W_k$  的順序(排列方法)无关。

$(0) \Rightarrow (i)$ . 假如把  $0 \in W$  分解为  $k$  个 0 成为  $0 = 0 + \dots + 0$  ( $0 \in W_i$ ), 就得到一个“0 的分解”( (4.4) 的意义), 但是由 (0) 它沒有其他的分解, 因此 (i) 成立。

$(i) \Rightarrow (ii)$ . 只要証明 (a) 假如  $W_1, \dots, W_{k-1}$  不无关, 那末 (i) 不成立, 及 (b) 假如  $(W_1 + \dots + W_{k-1}) \cap W_k \neq \{0\}$ , 那末 (i) 也不成立就行了。

(a) 如果  $W_1, \dots, W_{k-1}$  不无关, 那末  $W_1 + \dots + W_{k-1}$  中某个元能有两种分解, 因此  $x_1 + \dots + x_{k-1} = x'_1 + \dots + x'_{k-1}$ ,  $x_i, x'_i \in W_i$ ,  $i = 1, \dots, k-1$ , 并且对于某个  $i$ ,  $x_i \neq x'_i$ . 于是  $(x_1 - x'_1) + \dots + (x_{k-1} - x'_{k-1}) + 0 = 0$ ,  $x_i - x'_i \in W_i$ ,  $i = 1, \dots, k-1$ ,  $0 \in W_k$ , 所以 (i) 不成立。

(b) 由假設, 存在滿足  $(W_1 + \dots + W_{k-1}) \cap W_k \ni x_k \neq 0$  的  $x_k$ . 因为  $x_k \in W_k$ , 并且  $x_k \in W_1 + \dots + W_{k-1}$ , 所以可以写成  $x_k = x_1 + \dots + x_{k-1}$ ,  $x_i \in W_i$ ,  $i = 1, \dots, k-1$ . 于是  $x_1 + \dots + x_{k-1} - x_k = 0$ ,  $-x_k \neq 0$ , 因此 (i) 不成立。

(ii) $\Rightarrow$ (0). 假如  $x \in W_1 + \cdots + W_k$ , 由引理 1,  $x$  能够唯一地分解为  $x'_k + x_k$ ,  $x'_k \in W_1 + \cdots + W_{k-1}$ ,  $x_k \in W_k$  的形状。又因为  $W_1, \cdots, W_{k-1}$  是无关, 所以  $x'_k$  能够唯一地分解为  $x_1 + \cdots + x_{k-1}$  的形状。

(0) $\Rightarrow$ (iii). 由已經証明的 (0) $\Rightarrow$ (ii), 即得 (iii) 中  $i=k$  情形。由上面的注意, 因为在 (0),  $W_1, \cdots, W_k$  的顺序可以任意更換, 所以得到对于其他  $i$  的 (iii)。

(iii) $\Rightarrow$ (i). 假設  $x_1 + \cdots + x_k = 0$ , 如果  $x_k \neq 0$ , 因为  $x_1 + \cdots + x_{k-1} = -x_k \in (W_1 + \cdots + W_{k-1}) \cap W_k$ , 所以与 (iii) 矛盾。

(0) $\Rightarrow$ (iv). 由已經証明的 (0) $\Rightarrow$ (ii) 即得最后的  $(W_1 + \cdots + W_{k-1}) \cap W_k = \{0\}$ , 并且因为  $W_1, \cdots, W_{k-1}$  是无关, 又得到它前面的  $(W_1 + \cdots + W_{k-2}) \cap W_{k-1} = \{0\}$ , 余类推。

(iv) $\Rightarrow$ (i). 假定  $x_1 + \cdots + x_k = 0$  中的  $x_1, \cdots, x_k$  不完全是 0, 譬如它最后不为 0 的是  $x_j$ , 那末与 (iii) $\Rightarrow$ (i) 的証明同样就得到与  $(W_1 + \cdots + W_{j-1}) \cap W_j = \{0\}$  矛盾。

系 假定  $W_1, \cdots, W_k \in \mathfrak{B}^*$  无关, 那末  $W_{\nu_1}, \cdots, W_{\nu_l} (\{\nu_1, \cdots, \nu_l\} \subset \{1, \cdots, k\} l \leq k)$  也无关<sup>①</sup>。

例 8 在  ${}^nK$  中,  $[1e], \cdots, [ne]$  是无关。

## § 5 綫性无关,綫性相关,維数,基底

$K$  上向量空間  $V$  中异于 0 的元的集合  $V - \{0\}$  用  $V^*$  表示。假如  $x \in V^*$ , 显然  $[x] = \{\lambda x; \lambda \in K\} \in \mathfrak{B}^*$ . 所謂  $x_1, \cdots, x_k \in V^*$  綫性无关 (或簡称无关) 是意味着  $[x_1], \cdots, [x_k] \in \mathfrak{B}^*$  无关 (§4), 即  $[x_1, \cdots, x_k]$  中任意元  $x$  能够唯一地表示为  $\lambda_1 x_1 + \cdots + \lambda_k x_k$ ,  $\lambda_i \in K$

① 假如  $W_1, \cdots, W_l (l < k)$  相关, 由 (i) 就有滿足  $x_1 + \cdots + x_l = 0$  而  $x_1, \cdots, x_l$  不完全是 0 的元  $x_1, \cdots, x_l$ , 于是  $x_1 + \cdots + x_l + \underbrace{0 + \cdots + 0}_{k-l \text{ 个}} = 0$ , 这与  $W_1, \cdots, W_k$  无关的假設矛盾。——譯者注

的形状(特別只是一个  $x \in V^*$  总是无关的)。

对于  $W \in \mathfrak{B}^*$ ,  $x \in V^*$ , 显然

$$W \ni x \Leftrightarrow W \cap [x] = \{0\}.$$

据此, 由定理 1 立即得到下面的定理。

**定理 2** 向量空間  $V$  中异于 0 的元  $x_1, \dots, x_k$  ( $k$  是自然数  $\geq 2$ ) 成为綫性无关, 下面的 (i) ~ (iv) 都是它的必要充分条件。

(i)  $\lambda_1 x_1 + \dots + \lambda_k x_k = 0$ ,  $\lambda_i \in K \Rightarrow \lambda_i = 0$ ,  $i = 1, \dots, k$ .

(ii)  $x_1, \dots, x_{k-1}$  綫性无关,  $x_k \notin [x_1, \dots, x_{k-1}]$ .

(iii)  $x_i \notin [x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_k]$ ,  $i = 1, \dots, k$ .

(iv)  $x_2 \notin [x_1]$ ,  $x_3 \notin [x_1, x_2]$ ,  $\dots$ ,  $x_k \notin [x_1, \dots, x_{k-1}]$ .

**系** 假定  $x_1, \dots, x_k \in V^*$  无关, 那末  $x_{\nu_1}, \dots, x_{\nu_l}$  ( $\{\nu_1, \dots, \nu_l\} \subset \{1, \dots, k\}$ ,  $l \leq k$ ) 也无关。

**例 1** 在  ${}^n K$  中,  ${}_1 e, \dots, {}_n e$  是无关。

当  $x_1, \dots, x_k \in V$  不是綫性无关时,  $x_1, \dots, x_k$  叫做綫性相关或简称**相关**。特別是  $x_1, \dots, x_k$  中如果有一个是 0, 那末  $x_1, \dots, x_k$  相关。

**例 2**  $x_1, \dots, x_k$  相关意味着  $\lambda_1, \dots, \lambda_k$  中至少有一个不是 0 而  $\lambda_1 x_1 + \dots + \lambda_k x_k = 0$  成立。

**例 3** 在  $x_1, \dots, x_k$  ( $k \geq 2$ ) 中, 如果  $x_i = x_j$  ( $i \neq j$ ), 那末  $x_1, \dots, x_k$  相关。

**例 4** 假如  $x_1, \dots, x_{k-1}$  无关而  $x_1, \dots, x_{k-1}, x_k$  相关, 那末  $x_k \in [x_1, \dots, x_{k-1}]$ 。

**定理 3** 假定  $x_1, \dots, x_m$  是向量空間  $V$  中任意有限个元的集合, 那末除  $x_1 = \dots = x_m = 0$  的情形外, 能找到  $\{1, \dots, m\}$  的适当子集合  $\{\nu_1, \dots, \nu_k\}$  ( $1 \leq \nu_1 < \nu_2 < \dots < \nu_k \leq m$ ,  $k \leq m$ ), 使得下面的条件成立:

(i)  $x_{\nu_1}, \dots, x_{\nu_k}$  綫性无关。

(ii)  $[x_1, \dots, x_{\nu_1-1}] = [x_{\nu_1}]$ ,

$$[x_1, \dots, x_{\nu_1-1}] = [x_{\nu_1}, x_{\nu_1}],$$

.....

$$[x_1, \dots, x_m] = [x_{\nu_1}, x_{\nu_2}, \dots, x_{\nu_k}].$$

**证明** 自  $x_1, \dots, x_m$  中象下面那样挑选  $x_{\nu_1}, \dots, x_{\nu_k}$  即可。

假如  $x_1 \in V^*$  (即  $x_1 \neq 0$ ), 取  $\nu_1 = 1$ . 假如  $x_1 = 0$ , 把  $x_1, x_2, \dots$  中最初不是零的向量作为  $x_{\nu_1}$ . 于是

$$[x_1, \dots, x_{\nu_1}] = [x_{\nu_1}].$$

再假如  $x_{\nu_1}, x_{\nu_1+1}$  无关 (即  $x_{\nu_1+1} \notin [x_{\nu_1}]$ ), 取  $\nu_2 = \nu_1 + 1$ . 假如  $x_{\nu_1}, x_{\nu_1+1}$  相关, 把  $x_{\nu_1+1}, x_{\nu_1+2}, \dots$  中最初不在  $[x_{\nu_1}]$  中的向量作为  $x_{\nu_2}$ , 于是由定理 2 的 (iv),  $x_{\nu_1}, x_{\nu_2}$  无关,

$$[x_1, \dots, x_{\nu_2-1}] = [x_{\nu_1}],$$

$$[x_1, \dots, x_{\nu_2}] = [x_{\nu_1}, x_{\nu_2}].$$

余类推。

**定理 4** 假定  $x_1, \dots, x_k$  是向量空间  $V$  中任意有限个元的集合,  $y_1, \dots, y_h \in [x_1, \dots, x_k]$  ( $h \geq 1$ ), 并且  $y_1, \dots, y_h$  无关, 那末  $h \leq k$ , 并且可以挑选  $\{1, \dots, k\}$  的适当子集合  $\{\nu_1, \dots, \nu_h\}$ , 使得

$$1 \leq \nu_1 < \nu_2 < \dots < \nu_h \leq k,$$

$$[x_1, \dots, x_k] = [x_1, \dots, x_{\nu_1-1}, y_1, x_{\nu_1+1}, \dots,$$

$$\dots, x_{\nu_2-1}, y_2, x_{\nu_2+1}, \dots,$$

$$\dots$$

$$\dots, x_{\nu_h-1}, y_h, x_{\nu_h+1}, \dots, x_k].$$

**证明** 首先因为  $[x_1, \dots, x_k] \ni y_1 \neq 0$ , 的确  $k \geq 1$ , 并且不能有  $x_1 = \dots = x_k = 0$ . 再在  $y_1 = \lambda_1 x_1 + \dots + \lambda_k x_k$  的  $\lambda_1, \dots, \lambda_k$  中有不是 0 的。假如  $\lambda_{\nu_1}$  是其一, 那末

$$\begin{aligned} x_{\nu_1} &= \frac{1}{\lambda_{\nu_1}} y_1 = \frac{1}{\lambda_{\nu_1}} x_1 + \dots + \frac{\lambda_{\nu_1-1}}{\lambda_{\nu_1}} x_{\nu_1-1} \\ &\quad + \frac{\lambda_{\nu_1+1}}{\lambda_{\nu_1}} x_{\nu_1+1} + \dots + \frac{\lambda_k}{\lambda_{\nu_1}} x_k, \end{aligned}$$

即

$$x_{\nu_1} \in [x_1, \dots, x_{\nu_1-1}, y_1, x_{\nu_1+1}, \dots, x_k].$$



因而  $[x_1, \dots, x_k] = [x_1, \dots, x_{v_1-1}, y_1, x_{v_1+1}, \dots, x_k]$ .

其次, 假如  $k \geq 2$ ,  $y_2 \in [x_1, \dots, x_{v_1-1}, y_1, x_{v_1+1}, \dots, x_k]$  ( $y_1, y_2$  无关), 那末

$$y_2 = \mu_1 x_1 + \dots + \mu_{v_1-1} x_{v_1-1} + \mu_{v_1} y_1 + \mu_{v_1+1} x_{v_1+1} + \dots + \mu_k x_k,$$

因为这里  $\mu_1, \dots, \mu_{v_1-1}, \mu_{v_1+1}, \dots, \mu_k$  中一定有不是 0 的, 假如  $\mu_{v_1}$  是其一 (计算  $\mu$  的个数, 得知  $k-1 \geq 1$  即  $k \geq 2$ ), 那末

$$x_{v_1} = \frac{1}{\mu_{v_1}} y_2 - \frac{\mu_1}{\mu_{v_1}} x_1 - \dots - \frac{\mu_{v_1}}{\mu_{v_1}} y_1 - \dots - \frac{\mu_k}{\mu_{v_1}} x_k,$$

因而

$$x_{v_1} \in [x_1, \dots, x_{v_1-1}, y_1, x_{v_1+1}, \dots, x_{v_1-1}, y_2, x_{v_1+1}, \dots, x_k].$$

于是  $[x_1, \dots, x_k]$  与右边相等。

当  $k \geq 3$  时继续同样做即得。

**系 1**  $[x_1, \dots, x_k]$  中无关的向量的个数不大于  $k$ 。

**系 2** 假定  $x_1, \dots, x_k \in V$  无关<sup>①</sup>, 那末  $k$  是  $[x_1, \dots, x_k]$  中无关向量个数的最大数。

向量空间  $V$  所含无关向量的个数能够取任意多时 (即对于任意给定的自然数  $n$ ,  $V$  中有  $n$  个无关向量存在时)  $V$  叫做无限维。假如  $V$  不是无限维, 那末  $V$  所含无关向量的数有界。因而在个数中有最大数  $n$ , 这时  $V$  叫做有限维, 并且称  $n$  为它的维数 (dimension)。用记号  $\dim V = n$  表示。

假如  $\dim V = n$ ,  $V$  含有  $n$  个无关元  $x_1, \dots, x_n$ , 因为  $V$  中任意  $(n+1)$  个元不是无关, 所以假如  $x$  是  $V$  中任意元, 那末  $x_1, \dots, x_n, x$  成为相关。因而  $x \in [x_1, \dots, x_n]$  (例 4)。所以  $V = [x_1, \dots, x_n]$ , 即  $V$  是由  $x_1, \dots, x_n$  生成。象  $x_1, \dots, x_n$  这样,  $V$  中无关的生成元, 叫做  $V$  的基底。——总结以上即得下面定理。

**定理 5**  $n$  维向量空间有由  $n$  个向量构成的基底。

①  $x_1, \dots, x_k \in V$  无关隐含若  $x_1, \dots, x_k$  都不是 0, 即  $x_1, \dots, x_k \in V^*$  之意。

**例 5** 在  ${}^n K$  中,  $\{e_1, e_2, \dots, e_n\}$  成为一个基底. 在  $K^n$  中,  $\{e_1, e_2, \dots, e_n\}$  成为一个基底. 它们分别叫做  ${}^n K, K^n$  的自然基底.

**系 1**  $n$  维向量空间是  $n$  个 1 维空间的直和.

**证明** 假定  $\dim V = n$ , 因为  $V$  有由  $n$  个元构成的基底  $x_1, \dots, x_n$ , 所以  $V = [x_1, \dots, x_n] = [x_1] \oplus \dots \oplus [x_n]$ , 因为  $[x_i]$  有由一个元构成的基底, 所以它是 1 维的.

**系 2** 体  $K$  上  $n$  维向量空间与  ${}^n K$  同构.

**证明** 当  $\dim V = n$  时, 设  $V$  的基底是  $x_1, \dots, x_n$ , 那末  $x \in V$  可以唯一地写成  $\lambda_1 x_1 + \dots + \lambda_n x_n$  的形状. 这时命  $f(x) = (\lambda_1, \dots, \lambda_n) \in {}^n K$ , 显然  $f$  是自  $V$  到  ${}^n K$  的同构映射.

**例 6**  ${}^n K \cong K^n, {}^1 K \cong K^1 \cong K$  (参照 § 3 例 7).

**系 3** 假定  $W$  是  $V$  的子空间,  $\dim V = n, \dim W = m$ , 那末  $n \geq m$ , 这时如果  $n = m$ , 那末  $V = W$ .

**证明** 因为  $\dim V, \dim W$  分别是  $V, W$  中无关向量的最大个数, 显然  $V \supset W \Rightarrow n = \dim V \geq m = \dim W$ .

假定  $W$  的基底是  $x_1, \dots, x_m, W = [x_1, \dots, x_m]$ , 如果  $V \supsetneq W$ , 那就有含于  $V$  而不含于  $W$  的向量  $x_{m+1}$ , 这时  $x_1, \dots, x_m, x_{m+1}$  无关 (定理 2, (ii)), 所以  $n > m$ .

**系 4** 假定  $W$  是  $V$  的子空间,  $\dim V = n, \dim W = m, n > m$ , 如果  $x_1, \dots, x_m$  是  $W$  的一个基底, 那就可以添加  $n - m$  个向量  $x_{m+1}, \dots, x_n$ , 使  $x_1, \dots, x_n$  成为  $V$  的基底 (由定理 5 及定理 4).

**系 5** 在系 4 中, 假如  $W' = [x_{m+1}, \dots, x_n]$ , 那末  $V = W \oplus W'$ , 即  $V$  的任意子空间  $W$  是  $V$  的直和因子.

**证明** 因为  $V \ni x = \lambda_1 x_1 + \dots + \lambda_m x_m + \lambda_{m+1} x_{m+1} + \dots + \lambda_n x_n \in W + W'$ , 所以  $V = W + W'$ . 又假如  $W \ni y = \mu_1 x_1 + \dots + \mu_m x_m$ ,  $W' \ni y' = \mu_{m+1} x_{m+1} + \dots + \mu_n x_n$ , 如果  $y + y' = 0$ , 那末  $\mu_1 = \dots = \mu_n = 0$ , 所以  $y = y' = 0$ . 于是  $W, W'$  无关. 因此  $V = W \oplus W'$ . (证毕)

假定  $W$  是  $V$  的一个子空間, 对于  $x, y \in V$ , 如果  $x - y \in W$ , 那末  $x, y$  叫做关于  $\bmod W$  相合。写成  $x \equiv y \pmod{W}$ 。假如  $x \equiv 0, y \equiv 0 \pmod{W}$ , 显然  $x + y \equiv 0, \lambda x \equiv 0 \pmod{W}$ 。

$k$  个向量  $x_1, \dots, x_k$  满足

$$\lambda_1 x_1 + \dots + \lambda_k x_k \equiv 0 \pmod{W} \Rightarrow \lambda_1 = \dots = \lambda_k = 0$$

时, 叫做关于  $\bmod W$  綫性无关。

**命題 4** 假定  $x_1, x_2, \dots, x_k$  关于  $\bmod W$  綫性无关, 那末

- (i) 它們綫性无关。
- (ii) 它的任意子集合  $\{x_{\nu_1}, \dots, x_{\nu_k}\}$  也关于  $\bmod W$  綫性无关。
- (iii)  $x_i \notin W (i = 1, 2, \dots, k)$ 。

**証明** 由綫性无关及关于  $\bmod W$  綫性无关的定义即能容易地証明(今后, 容易的証明省略, 請讀者作为练习題来考虑)。

**定理 6** 假定  $V$  是向量空間,  $W$  是它的子空間, 如果  $\dim V = n, \dim W = m$ , 那末  $V$  中存在  $(n - m)$  个关于  $\bmod W$  綫性无关的向量。

**証明** 定理 5 系 4 中的  $(n - m)$  个向量  $x_{m+1}, \dots, x_n$  适合这条件。

**例 7** 假定  $W$  是  $V$  的一个固定子空間, 那末关于  $\bmod W$  的相合关系是等价关系。即  $x \equiv x; x \equiv y \Rightarrow y \equiv x; x \equiv y, y \equiv z \Rightarrow x \equiv z$  (在这些“相合式”中都把  $\bmod W$  省略)。当  $x \equiv y$  时,  $x$  关于  $\bmod W$  的相合类与  $y$  关于  $\bmod W$  的相合类叫做相同。 $x$  关于  $\bmod W$  的相合类用  $(x)_W$  或簡略地用  $(x)$  表示。因为  $x \equiv x', y \equiv y' \Rightarrow x + y \equiv x' + y', \lambda x \equiv \lambda x'$ , 所以由  $(x + y) = (x) + (y), (\lambda x) = \lambda(x)$  能够定义相合类的和及数量倍。假如这样定义, 那末相合类就成为  $K$  上向量空間。它叫做  $V$  关于  $\bmod W$  的商空間, 用  $V/W$  表示。特別, 如果  $\dim V = n, \dim W = m$ , 那末  $\dim V/W = n - m$  (定理 6 的証明中  $x_{m+1}, \dots, x_n$  的相合类  $(x_{m+1}), \dots, (x_n)$  构成  $V/W$  的基底)。

## §6 关于映射

作为 §2 的繼續, 在这里就映射或对应的概念及記法給予一

般的說明。

讀者想已知道象下面这样关于“函数”的定义。

“对于  $x$  的各个值, 对应的  $y$  值确定时,  $y$  叫做  $x$  的函数, 写成  $y=f(x)$ 。”

象这样說时,  $x, y$  当然认为是表示“数”, 所謂“数”就意味是普通实数(用我們的記法  $x, y \in R$ )。

依照函数  $f$ ,  $f(x)$  不一定定义于所有的实数(例如  $\sqrt{x}$  限于在实数范围内考虑时只有当  $x \geq 0$  时才有定义)。于是  $f(x)$  定义于某  $x$  的集合, 这样的集合叫做  $f$  的定义域(domain), 对于定义域

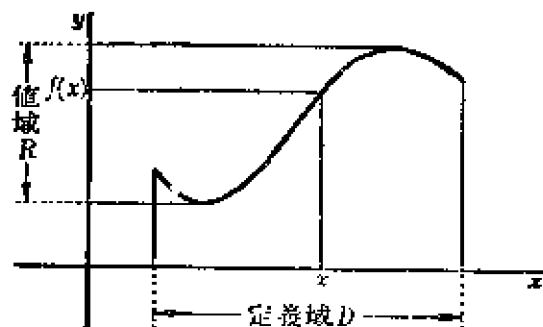


图 6.1

是  $D$  的函数  $f$ , 称  $R = \{f(x); x \in D\}$  为  $f$  的值域(range)。也有对于  $x$  的一个值确定两个以上  $f(x)$  的值的函数(象  $f(x) = \pm \sqrt{x}$ )称为多值函数。但今后为了简单, 只說函数时总是意味单值函数(不是多值的, 即对于  $x$  的一个值, 只确定一个唯一的  $f(x)$  的值)。

于 §2 中已注意到, 在我們的代数学中文字不一定表示数, 并且还說过, 代数学的对象是具有某种代数结构的集合, 即代数系。因此現在开始来考虑完全一般的集合。

假定  $M_1, M_2$  是两集合, 如果对于  $M_1$  中各个元  $x$ , 可以确定出  $M_2$  中元  $y$ , 这时, 我們就說給定了自  $M_1$  到  $M_2$  的映射或对应。这映射或对应用  $f$  表示时, 对于  $x \in M_1$  所确定(也叫做“对应”于  $x$ )的  $M_2$  中元  $y$  就用  $f(x)$  表示。

在微积分学中所討論的函数都是自  $M_1 = R$  到  $M_2 = R$  的映射(在复数函数論中考虑  $M_1 = M_2 = C$  的情况)。在一般集合情况也有仍旧使用函数这个名詞来代替映射或对应的, 但我們將以使用映射这个名詞为主。

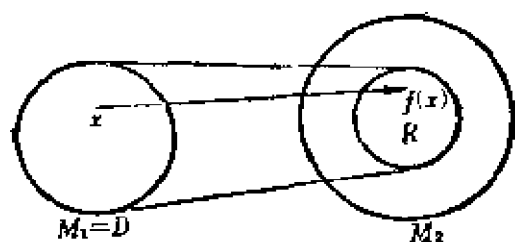


图 6.2

与函数的情况同样，也考虑“多值映射”。但当我们单说映射时，则规定是单值映射，即对于各个  $x \in M_1$ ， $f(x)$  是唯一确定的。又关于映射，也考虑定义域  $D \subset M_1$  及值域  $R \subset M_2$  的情况，但自“ $M_1$  到  $M_2$  的映射  $f$ ”，如果不预先声明，我们规定  $D = M_1$ ，即  $f(x)$  定义于  $M_1$  中所有元。然而常常不规定  $R = M_2$ ，特别，当  $R = M_2$  时， $f$  叫做（自  $M_1$ ）映成  $M_2$  的映射或到  $M_2$  的全射。为了表示  $f$  不一定是全射，常称它做（自  $M_1$ ）映入  $M_2$  中的映射。

**例 1** 假定  $y_0$  是  $M_2$  中一元，对于  $M_1$  中任意元  $x$ ，如果规定  $f(x) = y_0$ ，那就得到自  $M_1$  到  $M_2$  的一个映射。它叫做以  $y_0$  为值的常数映射。当  $M_2$  有两个以上之元时，它就不是全射。

**例 2** 假定  $M_1 = M_2 = M$ ，对于  $M$  中各个元  $x$  如果使  $x$  与  $x$  自身对应，那就得到自  $M$  到  $M$  自身的映射。它叫做关于  $M$  的恒等映射用  $e_M$  表示。 $e_M(x) = x$ ，恒等映射是全射。

当  $M_1 \supset M'_1$  时， $\{f(x); x \in M'_1\}$  是  $M_2$ （详细点说是  $R$ ）的子集合，写成  $f(M'_1)$ ，叫做  $M'_1$  关于  $f$  的象。（ $f(x)$  也叫做  $x$  的象，只由一个元构成的集合与这元自身常不加区别。）又  $M_2 \supset M'_2$  时， $\{x; f(x) \in M'_2\}$  是  $M_1$  的子集合，写成  $f^{-1}(M'_2)$ ，叫做  $M'_2$  的原象。对于  $y \in M_2$ ， $f^{-1}(\{y\})$ （ $\{y\}$  与  $y$  不加区别）写成  $f^{-1}(y)$ ，也叫做  $y$  的原象。 $f(x)$  是  $M_2$  中元，但  $f^{-1}(y)$  不是  $M_1$  中元而是  $M_1$  的子集合。假定  $M_2 \neq R$ ，如果  $y \in M_2 - R$ ，那末  $f^{-1}(y) = \emptyset$ 。对于  $y \in R$ ， $f^{-1}(y) \neq \emptyset$ ，假如对于  $R$  中任意元  $y$ ，如果  $f^{-1}(y)$  总是只由一个元构成时，那末  $f$  叫做一对一的映射或单射。假如  $f^{-1}(y) = \{x\}$ ，显然  $f(x) = y$ ，于是  $f^{-1}(y) = \{x\}$  时，如果写成  $f^{-1}(y) = x$ ，那末当  $f$  是单射时， $f^{-1}$  就是自  $R$  到  $M_1$  的全射。假如  $f$  是全射

同时又是单射,那末  $f$  叫做**全单射**。

**例3**  $M_1$  是由有限个元构成时,假定有自  $M_1$  到  $M_2$  的全单射,那末  $M_2$  是由相同个数的元所构成。

**例4**  $M_1 \supset M'_1 \supset M''_1 \Rightarrow R = f(M_1) \supset f(M'_1) \supset f(M''_1).$

$M_2 \supset M'_2 \supset M''_2 \Rightarrow M_1 = f^{-1}(M_2) \supset f^{-1}(M'_2) \supset f^{-1}(M''_2).$

**例5**  $M_2 \supset M'_2 \Rightarrow f^{-1}(M'_2) = f^{-1}(M'_2 \cap R).$

**例6**  $M_1 \supset M'_1 \Rightarrow f^{-1}(f(M'_1)) \supset M'_1$  ①.

**例7**  $M_2 \supset M'_2 \Rightarrow f(f^{-1}(M'_2)) \supset M'_2.$

設  $f$  是自  $M_1$  到  $M_2$  的映射,当  $M'_1 \subset M_1$  时,如果对于  $x \in M'_1$ , 使  $f(x) \in M_2$  与之对应,就得到自  $M'_1$  到  $M_2$  的映射。这映射叫做  $f$  到  $M'_1$  的**缩小**,用  $f| M'_1$  表示。与这相对,  $f$  有时叫做  $f| M'_1$  到  $M_1$  的**扩大**。显然由  $f$  能够确定  $f| M'_1$ , 但是由  $f| M'_1$  一般就不能确定  $f$ 。即当  $M_1 \supset M'_1$ ,  $M_1 \neq M'_1$  时,纵然  $f \neq g$ , 也可能有  $f| M'_1 = g| M'_1$ 。当  $M_1 = M'_1 \cup M''_1$  时,假如給定了  $f| M'_1$  及  $f| M''_1$ , 那末  $f$  就确定了。这些考虑在定义映射时或探求它的性质时将一再利用。

把自  $M_1$  到  $M_2$  的映射  $f$  表示为

$$f: M_1 \longrightarrow M_2 \quad \text{或} \quad M_1 \xrightarrow{f} M_2.$$

$f, g: M_1 \longrightarrow M_2$  意味着两个都是自  $M_1$  到  $M_2$  的映射。所謂  $f, g$  是相同映射 ( $f = g$ ), 当然是意味着对任意  $x \in M_1$  有  $f(x) = g(x)$ 。

假如  $f_1: M_1 \longrightarrow M_2, \quad f_2: M_2 \longrightarrow M_3,$

或  $M_1 \xrightarrow{f_1} M_2 \xrightarrow{f_2} M_3,$

对于  $x \in M_1$  使与  $f_2(f_1(x)) \in M_3$  对应,就得到自  $M_1$  到  $M_3$  的映射。用  $f_2 \circ f_1$  或簡略地用  $f_2 f_1$  表示。即

$$f_2 \circ f_1(x) = f_2 f_1(x) = f_2(f_1(x)).$$

---

① 因为  $f(M'_1)$  是  $M'_1$  关于  $f$  的象,  $f^{-1}(f(M'_1))$  是  $f(M'_1)$  的原象,显然它包含  $M'_1$  而被  $M_1$  包含,即  $M_1 \supset f^{-1}(f(M'_1)) \supset M'_1$ 。——譯者注

这  $f_2 \circ f_1$  叫做映射  $f_1, f_2$  的褶合。再由

$$M_1 \xrightarrow{f_1} M_2 \xrightarrow{f_2} M_3 \xrightarrow{f_3} M_4,$$

就得到自  $M_1$  到  $M_4$  的映射  $f_3 \circ (f_2 \circ f_1)$  及  $(f_3 \circ f_2) \circ f_1$ 。关于此,有

$$f_3 \circ (f_2 \circ f_1) = (f_3 \circ f_2) \circ f_1.$$

实际上,这两边相等是意味着对于任意  $x \in M_1$ ,

$$(f_3 \circ (f_2 \circ f_1))(x) = ((f_3 \circ f_2) \circ f_1)(x),$$

这两边显然都等于  $f_3(f_2(f_1(x)))$ 。这结果虽简单但很重要,故特列为下述定理。

**定理 7** 对于映射的褶合,結合律成立。

**例 8**  $f: M_1 \longrightarrow M_2$  时,  $f \circ e_{M_1} = f$ ,  $e_{M_2} \circ f = f$ 。

**例 9** 假定  $f: M_1 \longrightarrow M_2$  是全单射,那末  $f^{-1}: M_2 \longrightarrow M_1$  并且  $f^{-1} \circ f = e_{M_1}$ ,  $f \circ f^{-1} = e_{M_2}$ 。

**例 10** 假定在  $M_1 \xrightarrow{f_1} M_2 \xrightarrow{f_2} M_1 \xrightarrow{f_1} M_2$  中,  $f_2 \circ f_1 = e_{M_1}$ ,  $f_1 \circ f_2 = e_{M_2}$ , 那末  $f_1, f_2$  都是全单射<sup>①</sup>。

## §7 綫性映射

在前节是叙述完全一般集合間的映射,但是考虑代数系間的映射时,当然就要涉及到它的代数結構。

例如  $A_1, A_2$  是具有相同基本运算的代数系,并且在基本运算中有用“+”表示的加法。設  $f: A_1 \longrightarrow A_2$ , 对于  $A_1$  的任意两元  $x, y$ , 如果  $f(x+y) = f(x) + f(y)$ , 那末  $f$  叫做“保持加法”。保持所有基本运算的映射叫做同态映射。同态映射又是全单射时,就叫做同构映射。假如有自  $A_1$  到  $A_2$  的同构映射,那末  $A_1$  与  $A_2$  叫做同构。这事实都已在 §4 叙述过。

① 首先  $f_1, f_2$  都是全射,这是因为假如  $y$  是  $M_2$  中任意元,因为  $f_1 f_2 = e_{M_1}$ , 所以  $y \rightarrow f_2(y) \rightarrow f_1(f_2(y)) = y$ , 即  $y$  是  $M_1$  中元  $f_2(y)$  的象,所以  $f_1$  是全射。同样  $f_2$  也是全射。再假如  $x_1, x_2 \in M_1, f_1(x_1) = f_1(x_2)$ , 那末  $f_2 f_1(x_1) = f_2 f_1(x_2)$ , 即  $x_1 = x_2$ 。所以  $f_1, f_2$  都是单射。——譯者注

所謂綫性映射,不外是向量空間之間的同态映射。設  $V_1, V_2$  是同一个体  $K$  上的两向量空間,  $f$  是自  $V_1$  到  $V_2$  的映射,这时对于  $V_1$  的任意元  $x, y$  及  $K$  的任意元  $\lambda$ , 如果

$$f(x+y) = f(x) + f(y), \quad (7.1)$$

$$f(\lambda x) = \lambda f(x) \quad (7.2)$$

成立,那末  $f$  叫做自  $V_1$  到  $V_2$  的綫性映射<sup>①</sup>。自  $V_1$  到  $V_2$  的綫性映射全体的集合用  $\mathfrak{L}(V_1, V_2)$  表示。

**例 1** 向量空間  $V_1$  的恒等映射  $e_{V_1}$  是自  $V_1$  到它自身的綫性映射 (实际是同构映射):  $e_{V_1} \in \mathfrak{L}(V_1, V_1)$ 。

**例 2** 把  $V_1$  中任意元对应于  $V_2$  中元 0 的常数映射是  $\mathfrak{L}(V_1, V_2)$  中元, 这映射記为  $O_{V_1, V_2}$  或簡記为  $O$ 。

**例 3** 对于  ${}^nK$  中元  $(\xi_1, \dots, \xi_n)$ ,  $\xi_i \in K$ , 使它的第一坐标  $\xi_1$  对应的映射是  $\mathfrak{L}({}^nK, {}^1K)$  中元。这映射叫做“第一坐标上的射影”。同样, 对于  $i=2, 3, \dots, n$  定义“第  $i$  坐标上的射影”。这些都是  $\mathfrak{L}({}^nK, {}^1K)$  中元。

**例 4** 假定  $V = W_1 \oplus \dots \oplus W_k$ , 那末  $x \in V$  能够唯一地写成  $x_1 + \dots + x_k$ ,  $x_i \in W_i$  的形式, 这时, 对于  $x$ , 使与  $x_i$  对应的映射叫做自  $V$  到  $W_i$  的射影。它是  $\mathfrak{L}(V, W_i)$  中元 (例 3 是它的特殊情况)。

**例 5**  $W$  是  $V$  的子空間时, 对于  $x \in V$ , 使与  $(x)_W$  ( $x$  关于  $\text{mod } W$  的相合类, § 5, 例 7) 对应的映射叫做自  $V$  到商空間  $V/W$  的自然映射。它是  $\mathfrak{L}(V, V/W)$  中元。

**例 6** 假定  $(\nu_1, \nu_2, \dots, \nu_n)$  是  $(12 \dots n)$  的一个排列 (例如  $n=3$  时,  $(\nu_1 \nu_2 \nu_3) = (312)$  等)。这时对于  $K^n$  中元  $\begin{pmatrix} \xi_1 \\ \vdots \\ \xi_n \end{pmatrix}$ , 使与  $\begin{pmatrix} \xi_{\nu_1} \\ \vdots \\ \xi_{\nu_n} \end{pmatrix}$  对应的映射用  $\pi(\nu_1, \nu_2, \dots, \nu_n)$  表示, 它是  $\mathfrak{L}({}^nK^n, K^n)$  中元。特別,  $\pi(12 \dots n) = e_{K^n}$ 。

**例 7** 对于  $f \in \mathfrak{C}^1([a, b], \mathbf{R})$ , 使与它的导函数  $f' \in \mathfrak{C}^0([a, b], \mathbf{R})$  对应的映射  $D$  是自向量空間  $\mathfrak{C}^1$  到向量空間  $\mathfrak{C}^0$  的綫性映射,  $Df = f'$ ,  $D \in \mathfrak{L}(\mathfrak{C}^1, \mathfrak{C}^0)$ 。

① 綫性映射又叫做綫性作用素, 綫性运算符, 綫性算子。特別, 体  $K$  的綫性映射也叫做綫性泛函。



一般, 对于  $f \in \mathbb{C}^n([a, b], \mathbb{R})$ , 使与它的第  $k$  ( $k \leq n$ ) 阶导函数  $f^{(k)} \in \mathbb{C}^0([a, b], \mathbb{R})$  对应的映射用褶合映射的記法写成  $\underbrace{D \circ D \circ \cdots \circ D}_{(k \text{ 个})}$ , 簡記为  $D^k$ .

显然  $D^k \in \mathfrak{L}(\mathbb{C}^n, \mathbb{C}^0)$  ( $k \leq n$ ).

又当  $k \leq n$ ,  $p_1, p_2, \dots, p_k \in \mathbb{C}^0$  时, 由  $\Delta f = D^k f + p_1 D^{k-1} f + \cdots + p_{k-1} Df + p_k f$  定义的映射  $\Delta \in \mathfrak{L}(\mathbb{C}^n, \mathbb{C}^0)$ . 这  $\Delta$  表为  $\Delta = D^k + p_1 D^{k-1} + \cdots + p_{k-1} D + p_k$ .

**例 8** 对于  $f \in \mathbb{C}^0([a, b], \mathbb{R})$ , 使与  $\int_a^b f(x) dx \in \mathbb{R}$  对应的映射  $I$  是自向量空間  $\mathbb{C}^0$  到向量空間  $\mathbb{R}$  的綫性映射 (綫性泛函)

$$If = \int_a^b f(x) dx, \quad I \in \mathfrak{L}(\mathbb{C}^0, \mathbb{R}).$$

关于綫性映射, 下面的定理成立。

**定理 8** 假定  $f$  是自向量空間  $V_1$  到  $V_2$  的綫性映射,  $V'_1$  是  $V_1$  的子空間,  $V'_2$  是  $V_2$  的子空間, 那末  $f(V'_1)$  是  $V_2$  的子空間,  $f^{-1}(V'_2)$  是  $V_1$  的子空間。

設  $V_1, V_2$  的子空間的集合分別用  $\mathfrak{B}_1, \mathfrak{B}_2$  表示, 那末

$$\mathfrak{B}_1 \ni V'_1 \Rightarrow f(V'_1) \in \mathfrak{B}_2, \quad (7.3)$$

$$\mathfrak{B}_2 \ni V'_2 \Rightarrow f^{-1}(V'_2) \in \mathfrak{B}_1. \quad (7.4)$$

这意味着  $f: \mathfrak{B}_1 \rightarrow \mathfrak{B}_2$ ,  $f^{-1}: \mathfrak{B}_2 \rightarrow \mathfrak{B}_1$ . 特別,  $f(V_1) \in \mathfrak{B}_2$ ,  $f^{-1}(0) \in \mathfrak{B}_1$ .

**証明** 要証明 (7.3), 只要証明  $f(V'_1) \ni x', y' \Rightarrow x' + y', \lambda x' \in f(V'_1)$  即可。由  $f(V'_1)$  的定义, 存在  $x' = f(x)$ ,  $y' = f(y)$ ,  $x, y \in V'_1$  这样的  $x, y$ . 因为  $V'_1 \in \mathfrak{B}_1$ , 所以  $x + y, \lambda x \in V'_1$ . 又因为  $f \in \mathfrak{L}(V_1, V_2)$ , 所以  $x' + y' = f(x) + f(y) = f(x + y) \in f(V'_1)$ ,  $\lambda x' = \lambda f(x) = f(\lambda x) \in f(V'_1)$ . (7.4) 可同样地証明。

**例 9** 假定例 7 中的映射是  $D$ , 那末  $\Delta = D^n + p_1 D^{n-1} + \cdots + p_n \in \mathfrak{L}(\mathbb{C}^n, \mathbb{C}^0)$ . 对于  $\mathbb{C}^0$  的 0 向量 ( $f(x) = 0$  这样的函数  $f$ ),  $\Delta^{-1}(0)$  成为  $\mathbb{C}^n$  的子空間, 即  $n$  阶綫性微分方程

$$(D^n + p_1 D^{n-1} + \cdots + p_n)f = \frac{d^n f}{dx^n} + p_1 \frac{d^{n-1} f}{dx^{n-1}} + \cdots + p_n f = 0$$

的解集合是  $\mathbb{C}^n$  的子空間。

对于  $f, g \in \mathfrak{L}(V_1, V_2)$  及  $\lambda \in K$ , 定义  $f+g, \lambda f$  如下:  $f+g$  是使  $V_1$  的元  $x$  与  $V_2$  的元  $f(x)+g(x)$  对应的映射, 即

$$(f+g)(x) = f(x) + g(x),$$

而  $\lambda f$  是使  $V_1$  的元  $x$  与  $V_2$  的元  $\lambda f(x)$  对应的映射, 即

$$(\lambda f)(x) = \lambda f(x).$$

**命题 5** 对于上面定义加法及数量积,  $\mathfrak{L}(V_1, V_2)$  成为  $K$  上向量空间。

**証明** 証明 §3 中条件 A, B 在現在的情况下成立即可。例如 A1 可象下面这样来証明:

$$(f+g)(x) = f(x) + g(x) = g(x) + f(x) = (g+f)(x),$$

因为它对于任意  $x \in V_1$  成立, 所以  $f+g = g+f$ . 对于 A2~5, B1~5 也可同样验证。特別,  $\mathfrak{L}(V_1, V_2)$  中零元是以 0 为值的常数映射。

**命题 6** 假定  $f \in \mathfrak{L}(V_1, V_2)$ ,  $g \in \mathfrak{L}(V_2, V_3)$ , 那末  $g \circ f \in \mathfrak{L}(V_1, V_3)$ .

**証明** 显然  $g \circ f$  是由  $V_1$  到  $V_3$  的映射。由下面的关系即知它是綫性映射。

$$\begin{aligned} (g \circ f)(x+y) &= g(f(x+y)) = g(f(x) + f(y)) \\ &= g(f(x)) + g(f(y)) \\ &= (g \circ f)(x) + (g \circ f)(y), \\ (g \circ f)(\lambda x) &= g(f(\lambda x)) = g(\lambda f(x)) \\ &= \lambda g(f(x)) = \lambda (g \circ f)(x). \end{aligned}$$

**命题 7** 假定  $f, f_1, f_2 \in \mathfrak{L}(V_1, V_2)$ ,  $g, g_1, g_2 \in \mathfrak{L}(V_2, V_3)$ , 那末

$$g \circ (f_1 + f_2) = (g \circ f_1) + (g \circ f_2), \quad (7.5)$$

$$(g_1 + g_2) \circ f = (g_1 \circ f) + (g_2 \circ f). \quad (7.6)$$

**証明** 对于任意  $x \in V_1$ ,

$$\begin{aligned}
(g \circ (f_1 + f_2))(x) &= g((f_1 + f_2)(x)) \\
&= g(f_1(x) + f_2(x)) \\
&= (g \circ f_1)(x) + (g \circ f_2)(x) \\
&= (g \circ f_1 + g \circ f_2)(x),
\end{aligned}$$

所以(7.5)成立。(7.6)能够同样証明。(証毕)

在命題 5, 6, 7 中假如考虑  $V_1 = V_2 = V_3 = V$  的特殊情况, 那末,  $\mathfrak{L}(V, V)$  是  $K$  上向量空間, 对于其中任意两元  $f, g, g \circ f \in \mathfrak{L}(V, V)$ . 并且关于它的褶合及加法, 下面两个分配律

$$\begin{aligned}
h \circ (f + g) &= h \circ f + h \circ g, \\
(f + g) \circ h &= f \circ h + g \circ h \quad (f, g, h \in \mathfrak{L}(V, V))
\end{aligned}$$

成立。再对于任意  $\lambda \in K$ , 显然

$$\lambda(g \circ f) = (\lambda g) \circ f = g \circ (\lambda f).$$

一般, 在加群  $S$  中任意两元  $x, y$  之間定义异于“+”的算法“ $\circ$ ”而  $x \circ y \in S$ , 当

$$\begin{aligned}
&\text{結合律} && (x \circ y) \circ z = x \circ (y \circ z), \\
&\text{及分配律} && (x + y) \circ z = x \circ z + y \circ z, \\
&&& z \circ (x + y) = z \circ x + z \circ y
\end{aligned}$$

成立时,  $S$  叫做关于“+”, “ $\circ$ ”成为环。在环  $S$  中, 若更有

$$\text{交換律} \quad x \circ y = y \circ x,$$

則  $S$  就叫做可換环。 $x \circ y$  总是作为“乘法”, 表为  $xy$  的形状。可換环不外是加减乘法能够如常施行的集合(在 § 3 定义的体, 也可以說是“除法也能够如常施行的可換环”)。

体  $K$  上向量空間  $U$  当然是加群, 但  $U$  如果是环, 并且对于任意  $\lambda \in K, x, y \in U$ ,

$$\lambda(xy) = (\lambda x)y = x(\lambda y)$$

成立时, 則  $U$  叫做  $K$  上代数。

引用这定义, 上面所考察的事实可表达如次:

**命题 8** 如果  $V$  是  $K$  上向量空间, 则  $\mathfrak{L}(V, V)$  是  $K$  上代数。以后将  $\mathfrak{L}(V, V)$  写成  $\mathfrak{L}(V)$ 。  $\mathfrak{L}(V)$  中元也叫做  $V$  的线性变换。

**例 10** 整数全体的集合  $\{\pm n\}$ , 偶数全体的集合  $\{\pm 2n\}$ , 一般整数  $k$  的倍数全体的集合  $\{\pm kn\}$ , 按普通的加法乘法都成为环。上面两个环分别叫做整数环与偶数环。

**例 11** 在环中, 对于任意元  $x$ , 使  $ex = xe = x$  这样的元  $e$  (单位元) 不一定存在, 但是假如存在, 那就只有一个。

1 是整数环的单位元, 偶数环的单位元不存在。在  $\mathfrak{L}(V)$  中, 恒等映射  $e_V$  是单位元。

**例 12** 在有单位元  $e$  的环中, 对于任意元  $x$ , 象  $xx^{-1} = x^{-1}x = e$  这样的元  $x^{-1}$  ( $x$  的逆元) 不一定存在, 但如果存在, 那它对于  $x$  是唯一确定的 (更详细地说: 在  $xx' = e$  中, 如果存在  $x$  的逆元, 那末  $x'$  就是  $x$  的逆元)。在整数环, 对于异于 1 的元, 逆元不存在。在  $\mathfrak{L}(V)$ , 仅当  $f \in \mathfrak{L}(V)$  是全单射时,  $f$  的逆元存在,  $f^{-1}$  是它的逆元。

**例 13**  $C$  是以  $1, i = \sqrt{-1}$  做基底的  $R$  上二维向量空间, 并且是代数。(  $R$  自身当然是  $R$  上代数。一般, 体  $K$  自身可以看成  $K$  上代数。)

**例 14** 假定  $K$  是体,  ${}^4K$  的基底用  $\{1, i, j, k\}$  表示, 在  ${}^4K$  中元之间由下列关系定义乘法:

$$i^2 = j^2 = k^2 = -1, \quad ij = -ji = k, \quad jk = -kj = i, \quad ki = -ik = j.$$

一般, 当  $a = \alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k$ ,  $b = \beta_0 + \beta_1 i + \beta_2 j + \beta_3 k$  ( $\alpha_i, \beta_i \in K$ ) 时,

$$\begin{aligned} ab = & (\alpha_0\beta_0 - \alpha_1\beta_1 - \alpha_2\beta_2 - \alpha_3\beta_3) + (\alpha_0\beta_1 + \alpha_1\beta_0 + \alpha_2\beta_3 - \alpha_3\beta_2)i \\ & + (\alpha_0\beta_2 + \alpha_2\beta_0 + \alpha_3\beta_1 - \alpha_1\beta_3)j + (\alpha_0\beta_3 + \alpha_3\beta_0 + \alpha_1\beta_2 - \alpha_2\beta_1)k, \end{aligned}$$

那末  ${}^4K$  成为代数。这样的代数用  $Q(K)$  表示, 叫做体  $K$  上四元数环 (quaternion algebra)。在  $Q(K)$  中,  $1 = 1 + 0 \cdot i + 0 \cdot j + 0 \cdot k$  是单位元。

在  $Q(K)$  的元  $\alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k$  中,  $\alpha_1 = \alpha_2 = \alpha_3 = 0$  全体的集合关于加法乘法是与体  $K$  同构。因此, 假如把  $\alpha_0 + 0i + 0j + 0k \in Q(K)$  与  $\alpha_0 \in K$  “同样看待”, 那就可以认为  $Q(K) \supset K$ 。

对于  $a = \alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k \in Q(K)$ , 叫  $\bar{a} = \alpha_0 - \alpha_1 i - \alpha_2 j - \alpha_3 k$  做  $a$  的共轭元。由上面乘法定义, 容易得知

$$a\bar{a} = \bar{a}a = \alpha_0^2 + \alpha_1^2 + \alpha_2^2 + \alpha_3^2 \in K \text{ (在上述的意义)}。$$

特别, 假定  $K = \mathbf{R}$  而考虑  $Q(\mathbf{R})$ , 显然  $a = 0 \Rightarrow a\bar{a} = 0$ . 因此, 如果  $a \neq 0$ , 那末  $\frac{\bar{a}}{a\bar{a}} \in Q(K)$ ,  $\frac{\bar{a}}{a\bar{a}} \cdot a = a \cdot \frac{\bar{a}}{a\bar{a}} = 1$ , 即  $\frac{\bar{a}}{a\bar{a}}$  是  $a$  的逆元  $a^{-1}$ . 于是  $Q(\mathbf{R})$  除乘法的交换律之外满足体的公理, 象这样的体, 叫做**非可换体**(在较广泛的意义下, 也有把非可换体包含在内而统称为“体”的)。

代数成为体时, 叫做**可除代数**.  $\mathbf{R}$  上可除代数已知只有  $\mathbf{R}, \mathbf{C}, Q(\mathbf{R})$  三个(Frobenius 定理)①。

## § 8 矩陣表現

本节讨论有限维向量空间, 假定  $\dim V_1 = n$ ,  $\dim V_2 = m$ .

由 § 5 定理 5,  $V_1$  具有由  $n$  个元构成的基底  $a_1, a_2, \dots, a_n$ , 而  $V_1$  中每个元  $x$  能够唯一地表为  $\xi_1 a_1 + \dots + \xi_n a_n$ ,  $\xi_i \in K$  的形状。

假如对于  $x$ , 使  $K^n$  中元  $\begin{pmatrix} \xi_1 \\ \vdots \\ \xi_n \end{pmatrix}$  与之对应, 就得到自  $V_1$  到  $K^n$  的同

构映射。这同构映射用  $\varphi$  表示, 即

$$\varphi(x) = \begin{pmatrix} \xi_1 \\ \vdots \\ \xi_n \end{pmatrix},$$

$\varphi(x)$  叫做  $x$  关于基底  $(a_1, \dots, a_n)$  的**坐标**。在有必要表明基底时, 把  $\varphi$  写成  $\varphi(a_1, \dots, a_n)$ .  $\varphi$  叫做关于基底  $(a_1, \dots, a_n)$  的**坐标系**。同样, 假定  $V_2$  的一个基底是  $b_1, \dots, b_m$ , 由它确定的  $V_2$  的坐标系用  $\psi$  表示。

现在假定  $f \in \mathcal{L}(V_1, V_2)$ , 由前节命题 6,

$$\psi \circ f \circ \varphi^{-1} \in \mathcal{L}(K^n, K^m).$$

$$\begin{array}{ccc} V_1 & \xrightarrow{f} & V_2 \\ \varphi \downarrow & & \downarrow \psi \\ K^n & \xrightarrow{\psi \circ f \circ \varphi^{-1}} & K^m \end{array}$$

它是自  $K^n$  到  $K^m$  的映射, 用  $F$  表示。下面我们来考虑  $F$  具体的表现。

① 参阅 A. I. 库洛什著“高等代数教程”, 柯召译, 高等教育出版社出版, § 58. ———译者注

假定  $K^n$  的自然基底 (§ 6 例 5) 是  $e_1, e_2, \dots, e_n$ .  $K^n$  中一般元

$\begin{pmatrix} \xi_1 \\ \vdots \\ \xi_n \end{pmatrix}$  等于  $\sum_{i=1}^n \xi_i e_i$ . 由自然基底所确定的  $K^n$  的坐标系叫做自然

坐标系, 用  $\varphi_0$  表示。

$$\begin{aligned} F \begin{pmatrix} \xi_1 \\ \vdots \\ \xi_n \end{pmatrix} &= F \left( \sum_{k=1}^n \xi_k e_k \right) = \sum_{k=1}^n \xi_k F(e_k) \\ &= \sum_{k=1}^n \xi_k \psi(f(\varphi^{-1}(e_k))), \end{aligned}$$

由  $\varphi$  的意义, 显然  $\varphi(a_k) = e_k$ ,  $\varphi^{-1}(e_k) = a_k$ , 因此, 上式右边成为  $\sum_{k=1}^n \xi_k \psi(f(a_k))$ , 现在假定  $\psi(f(a_k))$ , 即  $f(a_k)$  关于  $(b_1, \dots, b_m)$  的坐标是

$$\psi(f(a_k)) = \begin{pmatrix} \alpha_{1k} \\ \alpha_{2k} \\ \vdots \\ \alpha_{mk} \end{pmatrix}, \quad \alpha_{ik} \in K, \quad (8.1)$$

那末

$$F \begin{pmatrix} \xi_1 \\ \xi_2 \\ \vdots \\ \xi_n \end{pmatrix} = \sum_{k=1}^n \xi_k \begin{pmatrix} \alpha_{1k} \\ \alpha_{2k} \\ \vdots \\ \alpha_{mk} \end{pmatrix} = \begin{pmatrix} \sum_{k=1}^n \alpha_{1k} \xi_k \\ \sum_{k=1}^n \alpha_{2k} \xi_k \\ \vdots \\ \sum_{k=1}^n \alpha_{mk} \xi_k \end{pmatrix},$$

即設

$$F \begin{pmatrix} \xi_1 \\ \xi_2 \\ \vdots \\ \xi_n \end{pmatrix} = \begin{pmatrix} \eta_1 \\ \eta_2 \\ \vdots \\ \eta_n \end{pmatrix} (f(x) \text{ 关于 } (b_1, \dots, b_n) \text{ 的坐标}), \quad (8.2)$$

那末

$$\eta_i = \sum_{k=1}^n \alpha_{ik} \xi_k \quad (i=1, 2, \dots, m). \quad (8.3)$$

于是  $F$  的具体形状, 可以用把 (8.1) 的  $n$  个  $m$  維纵向量横排成表

$$\begin{pmatrix} \alpha_{11} & \alpha_{12} & \cdots & \alpha_{1k} & \cdots & \alpha_{1n} \\ \alpha_{21} & \alpha_{22} & \cdots & \alpha_{2k} & \cdots & \alpha_{2n} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ \alpha_{i1} & \alpha_{i2} & \cdots & \alpha_{ik} & \cdots & \alpha_{in} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ \alpha_{m1} & \alpha_{m2} & \cdots & \alpha_{mk} & \cdots & \alpha_{mn} \end{pmatrix}, \quad \alpha_{ik} \in K \quad (8.4)$$

来給出, 因此 (8.2) 可表为

$$\begin{pmatrix} \alpha_{11} & \alpha_{12} & \cdots & \alpha_{1n} \\ \alpha_{21} & \alpha_{22} & \cdots & \alpha_{2n} \\ \vdots & \vdots & & \vdots \\ \alpha_{m1} & \alpha_{m2} & \cdots & \alpha_{mn} \end{pmatrix} \begin{pmatrix} \xi_1 \\ \xi_2 \\ \vdots \\ \xi_n \end{pmatrix} = \begin{pmatrix} \sum_{k=1}^n \alpha_{1k} \xi_k \\ \sum_{k=1}^n \alpha_{2k} \xi_k \\ \vdots \\ \sum_{k=1}^n \alpha_{mk} \xi_k \end{pmatrix}.$$

象 (8.4) 这种由  $K$  中元形成的表叫做  $K$  中  $(m, n)$  型矩陣, 行向量  $(\alpha_{i1}, \alpha_{i2}, \dots, \alpha_{in})$  叫做它的第  $i$  行。 (8.1) 的右边的列向量叫做它的第  $k$  列,  $\alpha_{ik}$  叫做它的  $(i, k)$  元素。特别,  $m=n$  的矩陣叫做  $n$  級方陣。在方陣  $(\alpha_{ik})$  中,  $\alpha_{11}, \alpha_{22}, \dots, \alpha_{nn}$  叫做主对角綫元素。又矩陣也常常用一个文字表示, 写成

$$F = \begin{pmatrix} \alpha_{11} & \alpha_{12} & \cdots & \alpha_{1n} \\ \alpha_{21} & \alpha_{22} & \cdots & \alpha_{2n} \\ \vdots & \vdots & & \vdots \\ \alpha_{m1} & \alpha_{m2} & \cdots & \alpha_{mn} \end{pmatrix} \quad \text{或} \quad F = (\alpha_{ik})_{m, n}.$$

两矩陣  $F = (\alpha_{ik})_{m, n}$ ,  $G = (\beta_{ik})_{m', n'}$ , 当  $m=m'$ ,  $n=n'$ ,  $\alpha_{ik} = \beta_{ik}$  ( $i=1, \dots, m$ ,  $k=1, \dots, n$ ) 时, 且限于这时叫做相等。

**例 1**  $K^n$  的第一坐标上的射影, 如果采取自然坐标可以用  $(1, n)$  型矩陣  $(1, 0, 0, \dots, 0)$  表示。

**例 2** 在前节例 6 中的  $\pi(\nu_1, \nu_2, \dots, \nu_n)$ , 如果采取  $K^n$  的自然坐标可以用  $(1, \nu_1), (2, \nu_2), \dots, (n, \nu_n)$  的各元素是 1, 而其他元素都是 0 的矩陣表示。这矩陣記为  $P(\nu_1, \nu_2, \dots, \nu_n)$ , 例如<sup>①</sup>

$$P(3, 1, 2) = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix},$$

特別,  $P(1, 2, \dots, n) = (\delta_{ik})$ , 但  $\delta_{ik} = \begin{cases} 1 & (i=k) \\ 0 & (i \neq k) \end{cases}$ ,  $\delta_{ik}$  叫做 **Kronecker** 的  $\delta$ -函数。 $(\delta_{ik})$  叫做  $n$  級单位矩陣, 用  $E_n$  (或簡略地用  $E$ ) 表示。

其次, 考虑与前节中所討論的綫性映射間算法对应的矩陣間的算法。

$K$  中元构成的  $(m, n)$  型矩陣全体的集合用  $\mathfrak{M}(m, n; K)$  表示。由上述方法, 对于任意  $f \in \mathfrak{L}(V_1, V_2)$ , 对应一个  $F \in \mathfrak{M}(m, n; K)$ 。(这里固定  $V_1, V_2$  的坐标系  $\varphi_1, \varphi_2$ , 以下暂时把  $\mathfrak{L}(V_1, V_2)$ ,  $\mathfrak{M}(m, n; K)$  分別略記为  $\mathfrak{L}, \mathfrak{M}$ .) 反之, 对于任意

$$G = \begin{pmatrix} \beta_{11} & \cdots & \beta_{1n} \\ \vdots & & \vdots \\ \beta_{m1} & \cdots & \beta_{mn} \end{pmatrix} \in \mathfrak{M},$$

只有一个  $g \in \mathfrak{L}$  存在, 适合

<sup>①</sup> 这时  $\pi(3, 1, 2)$ , 因为  $\xi_1 e_1 + \xi_2 e_2 + \xi_3 e_3 = \xi_3 e_3 + \xi_1 e_1 + \xi_2 e_2$ , 于是

$$f(e_1) = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \quad f(e_2) = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}, \quad f(e_3) = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$$

所以

$$F \leftarrow f = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}.$$

——譯者注



$$\psi(g(a_k)) = \begin{pmatrix} \beta_{1k} \\ \vdots \\ \beta_{mk} \end{pmatrix}, \text{ 即 } g(a_k) = \psi^{-1} \begin{pmatrix} \beta_{1k} \\ \vdots \\ \beta_{mk} \end{pmatrix},$$

$$k = 1, \dots, n. \quad (8.5)$$

实际上, 根据 (8.5), 对于任意  $x = \sum_{k=1}^n \xi_k a_k \in V_1$ ,  $g(x)$  由

$$g(x) = g\left(\sum_{k=1}^n \xi_k a_k\right) = \sum_{k=1}^n \xi_k g(a_k),$$

确定, 这样定义的  $g$  易知是线性映射。

于是, 上述的  $\mathfrak{L}$  与  $\mathfrak{M}$  之间的对应是一对一的。根据这对应, 当  $f \leftrightarrow F = (\alpha_{ik})$ ,  $g \leftrightarrow G = (\beta_{ik})$  时,  $f+g$ ,  $\lambda f \in \mathfrak{L}$  与  $\mathfrak{M}$  中怎样的矩阵对应?

关于这, 假定

$$\psi \circ f(a_k) = \begin{pmatrix} \alpha_{1k} \\ \vdots \\ \alpha_{mk} \end{pmatrix}, \quad \psi \circ g(a_k) = \begin{pmatrix} \beta_{1k} \\ \vdots \\ \beta_{mk} \end{pmatrix}, \quad k = 1, 2, \dots, n,$$

考虑  $(\psi \circ (f+g))(a_k)$ ,  $(\psi \circ (\lambda f))(a_k)$  即可。因为

$$(\psi \circ (f+g))(a_k) = \psi(f(a_k)) + \psi(g(a_k))$$

$$= \begin{pmatrix} \alpha_{1k} + \beta_{1k} \\ \vdots \\ \alpha_{mk} + \beta_{mk} \end{pmatrix},$$

$$(\psi \circ (\lambda f))(a_k) = \begin{pmatrix} \lambda \alpha_{1k} \\ \vdots \\ \lambda \alpha_{mk} \end{pmatrix},$$

所以

$$\begin{aligned} \psi(f+g)\psi^{-1} &= \begin{pmatrix} \alpha_{11} + \beta_{11} & \cdots & \alpha_{1n} + \beta_{1n} \\ \vdots & & \vdots \\ \alpha_{m1} + \beta_{m1} & \cdots & \alpha_{mn} + \beta_{mn} \end{pmatrix} \\ &= (\alpha_{ik} + \beta_{ik}), \end{aligned}$$

$$\psi(\lambda f)\varphi^{-1} = \begin{pmatrix} \lambda\alpha_{11} & \cdots & \lambda\alpha_{1n} \\ \vdots & & \vdots \\ \lambda\alpha_{m1} & \cdots & \lambda\alpha_{mn} \end{pmatrix} = (\lambda\alpha_{ik}).$$

特別, 假如  $\lambda=0$ , 那末

$$\psi \circ 0 \circ \varphi^{-1} = \begin{pmatrix} 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix}.$$

当  $F = (\alpha_{ik})$ ,  $G = (\beta_{ik})$  时,  $(\alpha_{ik} + \beta_{ik})$  写成  $F + G$ ,  $(\lambda\alpha_{ik})$  写成  $\lambda F$ . 又所有元素是 0 的  $(m, n)$  型矩陣用  $O_{mn}$  (或  $O$ ) 表示, 叫做  $((m, n)$  型的) 零矩陣。

假定  $\mathfrak{M}$  的元之間的加法及数量积象上面那样定义, 因为  $\mathfrak{L}$  与  $\mathfrak{M}$  之間的对应保存加法及数量积, 所以  $\mathfrak{M}$  成为与  $\mathfrak{L}$  同构的体  $K$  上向量空間。  $O_{mn}$  显然是  $\mathfrak{M}$  的零元。

**命题 9**  $\mathfrak{L}(V_1, V_2) \cong \mathfrak{M}(m, n; K)$ .

**命题 10** 假定  $\dim V_1 = n$ ,  $\dim V_2 = m$ , 那末  $\dim \mathfrak{L}(V_1, V_2) = mn$ .

**証明** 只要能够証明  $\dim \mathfrak{M}(m, n; K) = mn$  即可。假定  $E_{ik}$  只是  $(i, k)$  元素是 1, 其他元素都是 0 的  $(m, n)$  型矩陣, 因为  $mn$  个矩陣  $E_{11}, E_{12}, E_{13}, \cdots, E_{mn}$ , 根据定理 2 (i) 是无关的, 并且  $M$  中任意元能够表为它們的綫性組合, 所以它們成为  $M$  的基底。因此  $\dim \mathfrak{M}(m, n; K) = mn$ .

**例 3** 假定  $V_1 = V_2 = V$ ,  $\varphi = \psi$ ,  $\dim V = n$ , 那末  $\mathfrak{L}(V) \cong \mathfrak{M}(n, n; K)$ ,  $\dim \mathfrak{L}(V) = n^2$ . 在这同构对应中对应于  $\mathfrak{L}(V)$  的恒等映射  $e_1$  的矩陣是  $n$  次单位矩陣  $E_n$ .

再来看: 对于映射的褶合, 对应的又是怎样的矩陣? 假定  $\dim V_1 = n$ ,  $\dim V_2 = m$ ,  $\dim V_3 = l$ , 則

$$\mathfrak{L}(V_1, V_2) \ni f \leftrightarrow F = (\alpha_{ik}) \in \mathfrak{M}(m, n; K),$$

$$\mathfrak{L}(V_2, V_3) \ni g \leftrightarrow G = (\beta_{lk}) \in \mathfrak{M}(l, m; K).$$

如果  $V_1, V_2, V_3$  的坐标系分别为  $\varphi, \psi, \chi$ , 那末

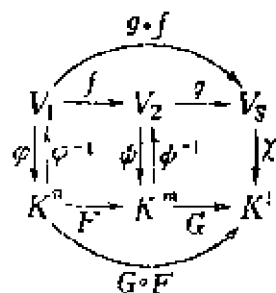
$$\chi((g \circ f)(a_k)) = \chi(g(f(a_k)))$$

$$= \chi\left(g\left(\sum_{j=1}^m \alpha_{jk} b_j\right)\right)$$

$$= \chi\left(\sum_{j=1}^m \alpha_{jk} g(b_j)\right)$$

$$= \sum_{j=1}^m \alpha_{jk} \chi(g(b_j))$$

$$= \sum_{j=1}^m \alpha_{jk} \begin{pmatrix} \beta_{1j} \\ \vdots \\ \beta_{lj} \end{pmatrix} = \begin{pmatrix} \sum_{j=1}^m \beta_{1j} \alpha_{jk} \\ \vdots \\ \sum_{j=1}^m \beta_{lj} \alpha_{jk} \end{pmatrix}, \quad k=1, 2, \dots, n.$$

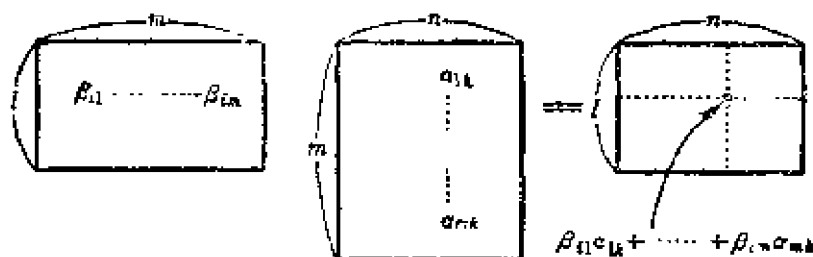


因此

$$\chi(g \circ f) \varphi^{-1} = \begin{pmatrix} \sum_{j=1}^m \beta_{1j} \alpha_{j1} & \cdots & \sum_{j=1}^m \beta_{1j} \alpha_{jn} \\ \vdots & & \vdots \\ \sum_{j=1}^m \beta_{lj} \alpha_{j1} & \cdots & \sum_{j=1}^m \beta_{lj} \alpha_{jn} \end{pmatrix} = \left( \sum_{j=1}^m \beta_{lj} \alpha_{jk} \right),$$

这矩阵叫做  $G = (\beta_{lk})$ ,  $F = (\alpha_{ik})$  的积, 写成  $GF$ .

矩阵的积只有第一个矩阵的列数与第二个矩阵的行数相等时才能定义。积的第  $(i, k)$  元素是第一个矩阵中第  $i$  行的元素与第二个矩阵中第  $k$  列的元素顺次相乘的和。



**命題 11** 当  $F, F_1, F_2 \in \mathfrak{L}(m, n; K)$ ,  $G, G_1, G_2 \in \mathfrak{M}(l, m; K)$  时,

$$\begin{aligned} G(F_1 + F_2) &= GF_1 + GF_2, \\ (G_1 + G_2)F &= G_1F + G_2F. \end{aligned}$$

**証明** 因为在  $\mathfrak{L}(V_1, V_2)$  与  $\mathfrak{L}(m, n; K)$ ,  $\mathfrak{L}(V_2, V_3)$  与  $\mathfrak{M}(l, m; K)$ ,  $\mathfrak{L}(V_1, V_3)$  与  $\mathfrak{M}(l, n; K)$  之間的一对一的对应, 保持加法及褶合(积), 并且关于  $\mathfrak{L}(V_1, V_2)$ ,  $\mathfrak{L}(V_2, V_3)$ ,  $\mathfrak{L}(V_1, V_3)$  中元命題 7 的关系成立, 所以上述的关系成立。

或引用矩陣的积及和的定义直接計算也容易驗證。

**命題 12**  $\mathfrak{M}(n, n; K)$  成为  $K$  上代数。作为代数也与  $\mathfrak{L}(V)$  同构。

以后  $\mathfrak{M}(n, n; K)$  簡写成  $\mathfrak{M}(n, K)$ 。

**例 4**  $\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 3 \\ 4 & 7 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} = \begin{pmatrix} 3 & 4 \\ 4 & 6 \end{pmatrix}.$

上例表示矩陣的乘法(即令只限于  $\mathfrak{M}(n, K)$  中元), 一般是不可交換的。因此, 对于  $\mathfrak{L}(V)$  中元間的褶合來說, 交換律不成立。

**例 5** 当  $G \in \mathfrak{M}(l, m; K)$ ,  $F \in \mathfrak{M}(m, n; K)$  时,  $F$  的  $n$  个列向量假定是  $a_1, a_2, \dots, a_n$ , 写成  $F = (a_1 \ a_2 \ \cdots \ a_n)$ , 那末由矩陣积的定义就得到

$$GF = G(a_1 \ a_2 \ \cdots \ a_n) = (Ga_1 \ Ga_2 \ \cdots \ Ga_n).$$

但  $Ga_i$  等是把  $a_i$  等看成  $(m, 1)$  型矩陣的积。假如把  $F$  中几个列向量集中写成  $F = (F_1 \ F_2)$ , 那末

$$GF = G(F_1 \ F_2) = (GF_1 \ GF_2). \quad (1)$$

同样, 若  $G$  的  $m$  个行向量是  ${}_1b, {}_2b, \dots, {}_mb$ , 把它們几个集中, 假如  $G = \begin{pmatrix} {}_1G \\ {}_2G \end{pmatrix}$ , 那末

$$GF = \begin{pmatrix} {}_1b \\ {}_2b \\ \vdots \\ {}_mb \end{pmatrix} F = \begin{pmatrix} {}_1bF \\ {}_2bF \\ \vdots \\ {}_mbF \end{pmatrix}, \quad GF = \begin{pmatrix} {}_1G \\ {}_2G \end{pmatrix} F = \begin{pmatrix} {}_1GF \\ {}_2GF \end{pmatrix}. \quad (2)$$

由(1), (2)得

$$GF = \begin{pmatrix} {}_1G \\ {}_2G \end{pmatrix} (F_1, F_2) = \begin{pmatrix} {}_1GF_1 & {}_1GF_2 \\ {}_2GF_1 & {}_2GF_2 \end{pmatrix}. \quad (3)$$

假如回到矩阵的定义来考虑,立刻知道

$$GF = (G_1 \ G_2) \begin{pmatrix} {}_1F \\ {}_2F \end{pmatrix} = G_{1 \ 1}F + G_{2 \ 2}F, \quad (4)$$

但是,在这里的划分要保証  $G_{1 \ 1}F$ ,  $G_{2 \ 2}F$  的积是可能的。以下同样。

由(3), (4)能够得到一般如下计算:

$$\begin{aligned} GF &= \begin{pmatrix} G_{11} & G_{12} \\ G_{21} & G_{22} \end{pmatrix} \begin{pmatrix} F_{11} & F_{12} \\ F_{21} & F_{22} \end{pmatrix} \\ &= \begin{pmatrix} G_{11}F_{11} + G_{12}F_{21} & G_{11}F_{12} + G_{12}F_{22} \\ G_{21}F_{11} + G_{22}F_{21} & G_{21}F_{12} + G_{22}F_{22} \end{pmatrix}. \end{aligned}$$

**例6** 把例2的  $P(v_1, v_2, \dots, v_m)$  写成  $\begin{pmatrix} v_1 e \\ v_2 e \\ \vdots \\ v_m e \end{pmatrix}$ , 如果

$$F = \begin{pmatrix} {}_1b \\ {}_2b \\ \vdots \\ {}_nb \end{pmatrix} \in \mathfrak{M}(m, n; K),$$

那末

$$P(v_1, v_2, \dots, v_m)F = \begin{pmatrix} v_1 b \\ v_2 b \\ \vdots \\ v_m b \end{pmatrix},$$

它是把  $F$  的行改排了。

同样,定义  $Q(v_1, v_2, \dots, v_m) = (e_{v_1}, e_{v_2}, \dots, e_{v_m})$ , 如果  $F = ({}_1a {}_2a \cdots {}_na)$ , 那末  $FQ(v_1, v_2, \dots, v_m) = ({}_1a {}_{v_1}a {}_{v_2}a \cdots {}_{v_m}a)$ . 它是把  $F$  的列改排了。

假定  $V_1 = V_2 = \cdots = V$ ,  $\dim V = n$ , 对于  $V$  取两种坐标系  $\varphi_1, \varphi_2$ , 那末

$$P = \varphi_2 \circ e_V \circ \varphi_1^{-1} \in \mathfrak{M}(n, n; K),$$

叫做自  $\varphi_1$  到  $\varphi_2$  的坐标变换的矩阵。假如

$$\begin{array}{c} V \xrightarrow{e_V} V \\ \varphi_1 \downarrow \uparrow \varphi_1^{-1} \downarrow \varphi_2 \\ K^n \xrightarrow{P} K^n \end{array}$$
  

$$\begin{array}{ccccccc} V & \xrightarrow{e_V} & V & \xrightarrow{e_V} & V & \xrightarrow{e_V} & V \\ \varphi_1^{-1} \downarrow & & \varphi_2 \downarrow & \varphi_2^{-1} \uparrow & \varphi_1 \downarrow & \varphi_1^{-1} \uparrow & \varphi_2 \downarrow \\ K^n & \xrightarrow{P} & K^n & \xrightarrow{P} & K^n & \xrightarrow{P} & K^n \\ & \searrow & \swarrow & \searrow & \swarrow & \searrow & \swarrow \\ & E & & E & & E & \end{array}$$

$\varphi_1 = \varphi_2$ , 象在例 3 中那样, 就得到  $P = E$ .

假定自  $\varphi_1$  到  $\varphi_2$  的坐标变换的矩阵是  $P$ , 自  $\varphi_2$  到  $\varphi_1$  的坐标变换的矩阵是  $\bar{P}$ , 那末

$$\bar{P}P = (\varphi_1 \circ e_V \circ \varphi_2^{-1}) \circ (\varphi_2 \circ e_V \circ \varphi_1^{-1}) = \varphi_1 \circ e_V \circ \varphi_1^{-1} = E.$$

同样,

$$P\bar{P} = \bar{P}P = E. \quad (8.6)$$

一般, 对于矩阵  $P$ , 如果存在使关系 (8.6) 成立的矩阵  $\bar{P}$ , 则称  $\bar{P}$  为  $P$  的逆矩阵, 今后用  $P^{-1}$  表示. 显然  $P$  是  $P^{-1}$  的逆矩阵. 具有逆矩阵的矩阵叫做正则矩阵. 正则矩阵是方阵.

**例 7** 假定  $F, G \in \mathfrak{M}(n, K)$ , 把  $E_n$  写成  $E$ , 那末

$$E^{-1} = E \quad (1), \quad FF - EF = F. \quad (2)$$

假如  $F, G$  是正则的, 那末  $FG$  也是正则的,  $(FG)^{-1} = G^{-1}F^{-1}$ . (3)

[解] (1), (2) 与命题 11 同样考虑, 或由矩阵的计算即得. (3) 由下面的关系自明.

$$\begin{aligned} (FG)(G^{-1}F^{-1}) &= F(GG^{-1})F^{-1} = E, \\ (G^{-1}F^{-1})(FG) &= G^{-1}(F^{-1}F)G = E. \end{aligned}$$

**例 8** 假定  $P(v_1, v_2, \dots, v_n), Q(v_1, v_2, \dots, v_n)$  是例 6 中的矩阵, 那末它们互为逆矩阵. 因而都是正则矩阵.

**命题 13** 假如两个向量空间  $V_1, V_2$  的坐标系分别由矩阵  $P, Q$  来变换, 那末对应于  $f \in \mathfrak{L}(V_1, V_2)$  的矩阵  $F$  就变成  $QFP^{-1}$ .

**证明** 从右边的图式即可明白。

**系** 假定  $\mathfrak{L}(V) \ni f \leftrightarrow F \in \mathfrak{M}(n, K)$ , 如果根据矩阵  $P$  施行  $V$  的坐标变换, 那末对应于  $f$  的矩阵就变成  $PF$ .

如果根据矩阵  $P^{-1}$  施行  $V$  的坐标变换, 那末对应于  $f$  的矩阵就变成  $P^{-1}F$ .

$$\begin{array}{ccccccc} V_1 & \xrightarrow{e_{V_1}} & V_1 & \xrightarrow{f} & V_2 & \xrightarrow{e_{V_2}} & V_2 \\ \varphi_2^{-1} \uparrow & & \varphi_1 \downarrow & & \varphi_1^{-1} \uparrow & & \psi_1 \downarrow \\ K^n & \xrightarrow{P^{-1}} & K^n & \xrightarrow{F} & K^n & \xrightarrow{Q} & K^n \end{array}$$

## §9 秩与退化次数

$f: V_1 \rightarrow V_2$  时,  $f(V_1)$  叫做  $f$  的象 (image). 写成  $\text{Im } f$ . 又

$f^{-1}(0)$  叫做  $f$  的核 (Kernel), 写成  $\text{Ker } f$ , 即

$$\text{Im } f \subset V_2, \text{Ker } f \subset V_1.$$

**命题 14**  $f$  是全射的必要充分条件是  $\text{Im } f = V_2$ . 又  $f$  是单射的必要充分条件是  $\text{Ker } f = \{0\}$ .

**证明** 前半段是显然的。后半段必要条件也是明显的。至于充分条件, 当  $\text{Ker } f = 0$  时, 假如  $x, y \in V_1, f(x) = f(y)$ , 那末  $f(x) - f(y) = f(x - y) = 0$ , 因此由  $x - y = 0$  就可以明白。(证毕)

当  $V_1, V_2$  是有限维时,  $\dim(\text{Im } f), \dim(\text{Ker } f)$  当然也是有限。它们分别叫做  $f$  的秩 (rank) 和退化次数 (degeneracy, nullity), 分别用  $r(f), d(f)$  表示。假如  $\dim V_1 = n, \dim V_2 = m$ , 那末  $0 \leq r(f) \leq m, 0 \leq d(f) \leq n$ . 特别, 假如把  $\mathfrak{L}(K^n, K^m)$  中元作为  $f$  来考虑, 那末矩阵  $F$  的秩  $r(F)$  和退化次数  $d(F)$  都有定义。

**命题 15**  $f$  是全射的必要充分条件是  $r(f) = m$ .  $f$  是单射的必要充分条件是  $d(f) = 0$ .

**证明** 由命题 14 自明。 (证毕)

假定  $f: V_1 \rightarrow V_2$  由某坐标系用矩阵  $F \in \mathfrak{M}(m, n; K)$  来表示。  $V_1 = [a_1, a_2, \dots, a_n]$ , 因为  $f(V_1) = [f(a_1), f(a_2), \dots, f(a_n)]$ , 所以  $r(f) = \dim f(V_1)$  等于  $f(a_1), f(a_2), \dots, f(a_n)$  中无关向量的个数。因而下面的命题成立。

**命题 16** 假定  $F$  是表示  $f$  的任意矩阵, 那末  $r(f) = r(F)$ . 并且它等于  $F$  的列向量中无关的个数。

**引理 2**  $r(f) \leq \min(m, n)$ .

**证明**  $r(f) \leq m$  在前面已明示。

再在  $f(V_1)$  中假定  $\{f(x_1), \dots, f(x_r)\}$  线性无关, 那末当  $\lambda_1 x_1 + \dots + \lambda_r x_r = 0$  时,  $0 = f(\lambda_1 x_1 + \dots + \lambda_r x_r) = \lambda_1 f(x_1) + \dots + \lambda_r f(x_r)$ , 所以  $\lambda_1 = \dots = \lambda_r = 0$ . 因此, 在  $V_1$  中  $\{x_1, \dots, x_r\}$  线性无关, 所以  $r(f) \leq n$ .

这引理的結論,詳言之,就有下面的定理9。

**定理9** 由向量空間  $V_1$  到  $V_2$  的綫性映射  $f$  的秩与退化次数的和等于  $\dim V_1$ 。

**証明** 假定  $\dim V_1 = n$ ,  $r(f) = r$ ,  $d(f) = d$ , 命  $n - d = r'$ , 証明  $r = r'$  即可。設

$$\text{Ker } f = [a_1, a_2, \dots, a_d],$$

那末表  $V_1 = [a_1, a_2, \dots, a_d, b_1, b_2, \dots, b_{r'}]$

时,由定理6的証明,  $\{b_1, b_2, \dots, b_{r'}\}$  关于  $\text{mod Ker } f$  綫性无关, 因而如果

$$\lambda_1 f(b_1) + \lambda_2 f(b_2) + \dots + \lambda_{r'} f(b_{r'}) = 0,$$

那末  $f(\lambda_1 b_1 + \lambda_2 b_2 + \dots + \lambda_{r'} b_{r'}) = 0$ , 于是  $\lambda_1 b_1 + \lambda_2 b_2 + \dots + \lambda_{r'} b_{r'} \in \text{Ker } f$ , 所以  $\lambda_1 = \lambda_2 = \dots = \lambda_{r'} = 0$ , 因此  $r'$  个向量  $f(b_1), \dots, f(b_{r'})$  是綫性无关。因为它們都  $\in f(V_1)$ , 所以  $r' \leq r$ 。

再假定任意  $x \in V_1$ , 因为能够表  $x = \lambda_1 a_1 + \dots + \lambda_d a_d + \mu_1 b_1 + \dots + \mu_{r'} b_{r'}$ , 所以  $f(x) = \mu_1 f(b_1) + \dots + \mu_{r'} f(b_{r'}) \in [f(b_1), \dots, f(b_{r'})]$ . 于是  $f(V_1) \subset [f(b_1), \dots, f(b_{r'})]$ . 但  $f(b_1), \dots, f(b_{r'})$  是綫性无关, 所以  $r \leq r'$ 。

于是  $r = r'$  即  $r + d = n$ 。

**系**  $f$  是单射的必要充分条件是  $r(f) = \dim V_1$ . 又  $f$  是全单射的必要充分条件是  $r(f) = \dim V_1 = \dim V_2$  (由命題15及定理9)。

$n$  級方阵  $K$  是正則的必要充分条件是  $r(K) = n$ . (系毕)

引用定理9的記法,假定

$$\text{Ker } f = [a_1, \dots, a_d],$$

$$V_1 = [b_1, \dots, b_r, a_1, \dots, a_d], \quad (9.1)$$

因为  $f(b_1), \dots, f(b_r)$  綫性无关, 所以在  $V_2$  中能够取得含有它們的基底



$$V_2 = [f(b_1), \dots, f(b_r), c_1, \dots, c_{m-r}]. \quad (9.2)$$

假定  $V_1, V_2$  的基底取如 (9.1), (9.2) 那样, 试来确定各个坐标系, 显然

$$f \leftrightarrow F = \left( \begin{array}{c|c} E_r & O_{m,n-r} \\ \hline O_{m-r,r} & \end{array} \right). \quad (9.3)$$

当  $V_1, V_2$  给以任意坐标时, 如果对于 (9.1), (9.2) 的坐标系施行坐标变换, 那末  $F$  能够变为 (9.3) 的形状。因此下面的定理成立。

**定理 10** 假定  $F \in \mathfrak{M}(m, n; K)$ , 如果  $r(F) = r$ , 那就能够挑选适当的正则矩阵  $P \in \mathfrak{M}(n, K)$ ,  $Q \in \mathfrak{M}(m, K)$ , 使得

$$QFP^{-1} = \left( \begin{array}{c|c} E_r & O_{m,n-r} \\ \hline O_{m-r,r} & \end{array} \right).$$

**例 1** 
$$F = \begin{pmatrix} -8 & 9 & -5 & 1 \\ 6 & -3 & 3 & -3 \\ -2 & 1 & 1 & 1 \end{pmatrix},$$

因为 
$$\begin{pmatrix} -8 \\ 6 \\ -2 \end{pmatrix} = \frac{3}{2} \begin{pmatrix} -5 \\ 3 \\ -1 \end{pmatrix} - \frac{1}{2} \begin{pmatrix} 1 \\ -3 \\ 1 \end{pmatrix}, \quad \begin{pmatrix} 9 \\ -3 \\ 1 \end{pmatrix} = -2 \begin{pmatrix} -5 \\ 3 \\ -1 \end{pmatrix} - \begin{pmatrix} 1 \\ -3 \\ 1 \end{pmatrix},$$

所以  $r(F) = 2$ , 命

$$Q = \begin{pmatrix} 0 & \frac{2}{5} & \frac{1}{5} \\ 1 & -\frac{1}{5} & -\frac{1}{10} \\ 2 & -\frac{1}{5} & -\frac{3}{5} \\ 0 & -\frac{1}{5} & -\frac{3}{5} \end{pmatrix}, \quad P^{-1} = \begin{pmatrix} 3 & 1 & 0 & 2 \\ 2 & 1 & 1 & 1 \\ -1 & 0 & 2 & -1 \\ 2 & 1 & 1 & 2 \end{pmatrix},$$

那末

$$QFP^{-1} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

**例 2**  $r(g \circ f) \leq \min(r(f), r(g)).$

[解] 假定  $V_1 \xrightarrow{f} V_2 \xrightarrow{g} V_3$ , 那末  $r(g \circ f) = \dim g(f(V_1)) \leq \dim f(V_1) = r(f)$ , 又

$$r(g \circ f) = \dim g(f(V_1)) \leq \dim g(V_2) = r(g).$$

例 3 假如把例 2 的结果就矩阵来叙述, 那就是  $r(GF) \leq \min(r(F), r(G))$ . 特别, 如果  $P$  是正则的, 那末  $r(PF) = r(FP) = r(F)$ .

[解] 当  $P$  是正则时, 取  $PF = G$ , 那末  $r(G) \leq r(F)$ , 因为  $F = P^{-1}G$ , 所以  $r(F) \leq r(G)$ . 于是  $r(PF) = r(F)$ . 同样,  $r(FP) = r(F)$ .

## § 10 对偶空间与转置映射

当  $V$  是体  $K$  上向量空间时,  $\mathfrak{L}(V, K)$  也是体  $K$  上向量空间。它叫做  $V$  的对偶空间, 用  $\hat{V}$  表示。

假定  $\dim V = n$ , 那末  $\dim \hat{V} = n$  ①. 取  $V$  的一个基底  $\{a_1, a_2, \dots, a_n\}$ , 给出坐标系  $\varphi = \varphi_{(a_1, a_2, \dots, a_n)}$ , 这时取  $\xi_i(a_j) = \delta_{ij}$  这样的  $n$  个  $\hat{V}$  中元  $\xi_1, \xi_2, \dots, \xi_n$ , 那末它们线性无关②. 实际上, 如果  $\lambda_1 \xi_1 + \dots + \lambda_n \xi_n = 0$ , 那就得到  $0 = (\lambda_1 \xi_1 + \dots + \lambda_n \xi_n)(a_j) = \lambda_j$ . 同样得到  $\lambda_2 = \lambda_3 = \dots = \lambda_n = 0$ . 因此  $\{\xi_1, \xi_2, \dots, \xi_n\}$  构成  $\hat{V}$  的基底。这  $\{\xi_1, \xi_2, \dots, \xi_n\}$  叫做  $\{a_1, a_2, \dots, a_n\}$  的对偶基底, 用  $\xi_i = \hat{a}_i$  表示。又这基底所确定的坐标系 ( $\varphi$  的对偶坐标系) 用  $\hat{\varphi}$  表示。

$$\begin{array}{ccc} V & \longrightarrow & \hat{V} \\ \downarrow \varphi & & \updownarrow \hat{\varphi} \\ K^n & \xrightarrow{E_{K^n}} & K^n \\ \varphi(a_i) = e_i & & \hat{\varphi} = \{\hat{a}_1, \dots, \hat{a}_n\} \\ & & \hat{a}_i(a_j) = \delta_{ij} \end{array}$$

因为由任意一对  $x \in V$  及  $\xi \in \hat{V}$  确定  $\xi(x) \in K$ , 把  $\xi(x)$  写成  $(x, \xi)$ , 于是  $x$  能够看成是自  $\hat{V}$  到  $K$  的映射。显然下面关系成立。

① 因为  $\dim V = n$ ,  $\dim K = 1$ , 由命题 10,  $\dim \hat{V} = \dim(V, K) = n \cdot 1 = n$ .  
——译者注

② 只是在此处,  $\xi, \xi_i$  (希腊字) 暂时不是表示  $K$  中元, 而是表示  $\hat{V} = \mathfrak{L}(V, K)$  中元。稍后  $\mathfrak{L}(V, K)$  中元将用  $\tau$  表示。

$$(x+y, \xi) = (x, \xi) + (y, \xi), (\lambda x, \xi) = \lambda(x, \xi),$$

$$(x, \xi+\eta) = (x, \xi) + (x, \eta), (x, \lambda\xi) = \lambda(x, \xi),$$

$$\left( \begin{array}{l} x, y \in V_1, \\ \xi, \eta \in V_1, \end{array} \lambda \in K \right).$$

这后面两式表示  $x \in V$  看成自  $\hat{V}$  到  $K$  的映射时, 它是綫性映射。  
即  $V \subset \mathfrak{L}(\hat{V}, K) = \hat{\hat{V}}$ .

**命题 17**  $V$  是  $\hat{V}$  的对偶空間。并且  $\{a_1, a_2, \dots, a_n\}$  成为  $(\hat{a}_1, \hat{a}_2, \dots, \hat{a}_n)$  的对偶基底。即

$$\hat{\hat{V}} = V, \quad \hat{\hat{a}}_i = a_i.$$

**証明** 証明前半段只要示明  $\hat{\hat{V}} \subset V$ , 即取任意  $\tau \in \mathfrak{L}(\hat{V}, K)$ , 示明存在  $\tau(\xi) = (x, \xi)$  ( $\xi \in \hat{V}$ ) 这样的  $x \in V$  即可。因为  $\tau(\hat{a}_i) \in K$  ( $i=1, 2, \dots, n$ ), 如果命

$$x = \tau(\hat{a}_1)a_1 + \tau(\hat{a}_2)a_2 + \dots + \tau(\hat{a}_n)a_n \in V,$$

那末对于这  $x$ ,

$$\begin{aligned} (x, \hat{a}_i) &= \tau(\hat{a}_1)(a_1, \hat{a}_i) + \tau(\hat{a}_2)(a_2, \hat{a}_i) + \dots \\ &\quad + \tau(\hat{a}_n)(a_n, \hat{a}_i) \\ &= \tau(\hat{a}_i), \quad i=1, 2, \dots, n. \end{aligned}$$

因为  $\{\hat{a}_1, \hat{a}_2, \dots, \hat{a}_n\}$  是  $\hat{V}$  的基底, 所以对于任意  $\xi \in \hat{V}$ ,  $(x, \xi) = \tau(\xi)$  ①.

后半段由  $(a_i, \hat{a}_j) = \delta_{ij}$  ② 自明。

假定  $W$  是  $V$  的子空間, 那末

① 因为  $\{\hat{a}_1, \dots, \hat{a}_n\}$  是  $\hat{V}$  的基底, 所以任意  $\xi \in \hat{V}$  可以写成

$$\xi = \lambda_1 \hat{a}_1 + \dots + \lambda_n \hat{a}_n,$$

于是

$$\begin{aligned} \tau(\xi) &= \lambda_1 \tau(\hat{a}_1) + \dots + \lambda_n \tau(\hat{a}_n) = \lambda_1 (x, \hat{a}_1) + \dots + \lambda_n (x, \hat{a}_n) \\ &= (x, \lambda_1 \hat{a}_1) + \dots + (x, \lambda_n \hat{a}_n) = (x, \lambda_1 \hat{a}_1 + \dots + \lambda_n \hat{a}_n) \\ &= (x, \xi). \end{aligned}$$

——譯者注

② 因为  $\xi_i(a_j) = \delta_{ij}$ ,  $\xi_i = \hat{a}_i$ , 所以  $(a_j, \xi_i) = (a_j, \hat{a}_i) = \delta_{ij}$  即  $(a_i, \hat{a}_j) = \delta_{ij}$ . 这就是說  $a_i$  把  $\hat{a}_i$  变为 1, 把  $\hat{a}_j$  变为 0, 所以  $a_i = \hat{\hat{a}}_i$ . ——譯者注

$$W' = \{\xi; \xi(W) = \{0\}\} \subset \hat{V},$$

叫做  $W$  的零化空间 (annihilator)。当  $\dim V = n$  时, 下面的命题成立。

**命题 18**  $(W')' = W, \dim W + \dim W' = n.$

**证明** 假定  $\dim W = r, W = [a_1, a_2, \dots, a_r], V = [a_1, \dots, a_r, a_{r+1}, \dots, a_n].$  引用它的对偶基底,  $\hat{V} = [\hat{a}_1, \dots, \hat{a}_r, \hat{a}_{r+1}, \dots, \hat{a}_n],$  于是  $\xi \in W' \Leftrightarrow \xi(a_i) = 0, i = 1, 2, \dots, r,$

假如命  $\xi = \lambda_1 \hat{a}_1 + \lambda_2 \hat{a}_2 + \dots + \lambda_n \hat{a}_n,$  那末  $(a_i, \xi) = \sum_{j=1}^n \lambda_j (a_i, \hat{a}_j).$

因此  $\xi(a_i) = (a_i, \xi) = 0 (i = 1, 2, \dots, r) \Leftrightarrow \lambda_1 = \lambda_2 = \dots = \lambda_r = 0,$  又显然  $\lambda_1 = \lambda_2 = \dots = \lambda_r = 0 \Leftrightarrow \xi \in [\hat{a}_{r+1}, \dots, \hat{a}_n].$  因此

$$\xi \in W' \Leftrightarrow \xi \in [\hat{a}_{r+1}, \dots, \hat{a}_n],$$

所以

$$W' = [\hat{a}_{r+1}, \dots, \hat{a}_n].$$

由此命题显然成立 ①。

例 1  $W_1 \supset W_2 \Leftrightarrow W'_1 \subset W'_2.$

例 2  $\{0\}' = \hat{V}, V' = \{0\}.$

其次, 假定  $f \in \mathfrak{L}(V_1, V_2),$  对于任意  $\xi \in \hat{V}_2,$  得知  $\xi \circ f \in \hat{V}_1.$  于是对于  $\xi$  使与  $\xi \circ f$  对应的映射用  ${}^t f$  表示, 叫做  $f$  的转置映射。由下面的关系得知  ${}^t f$  是线性映射:  ${}^t f \in \mathfrak{L}(\hat{V}_2, \hat{V}_1), {}^t f(\xi) = \xi \circ f,$

$$\begin{array}{ccccc} V_1 & \xrightarrow{f} & V_2 & \xrightarrow{\xi} & K \\ & & & \searrow & \\ & & & \xi \circ f & \end{array}$$

$$(\xi + \eta) \circ f = \xi \circ f + \eta \circ f, (\lambda \xi) \circ f = \lambda(\xi \circ f).$$

假定  $\dim V_1 = n, \dim V_2 = m,$  对于  $V_1, V_2$  给定坐标系  $\varphi, \psi, f$  用矩阵  $F$  表示, 同时对于  $\hat{V}_1, \hat{V}_2$  给出它们的对偶坐标系  $\hat{\varphi}, \hat{\psi}, {}^t f$  用矩阵  ${}^t F$  表示, 那末  ${}^t F$  叫做  $F$  的转置矩阵。

$$\begin{array}{ccc} V_1 & \xrightarrow{f} & V_2 \\ \varphi \downarrow & & \downarrow \psi \\ K^n & \xrightarrow{F} & K^m \end{array} \quad \begin{array}{ccc} \hat{V}_1 & \xrightarrow{{}^t f} & \hat{V}_2 \\ \hat{\varphi} \downarrow & & \downarrow \hat{\psi} \\ K^n & \xleftarrow{{}^t F} & K^m \end{array}$$

**命题 19** 假定  $F = (\alpha_{ik}),$  那末

① 因为  $W = [a_1, \dots, a_r], W' = [\hat{a}_{r+1}, \dots, \hat{a}_n], \hat{V} = [\hat{a}_1, \dots, \hat{a}_r, \hat{a}_{r+1}, \dots, \hat{a}_n],$  所以  $(W')' = [\hat{\hat{a}}_1, \dots, \hat{\hat{a}}_r] = [a_1, \dots, a_r] = W.$  ——译者注

$${}^tF = (\alpha_{ki}).$$

即  ${}^tF$  是互換  $F$  的行列所成的矩陣。如果

$$F = \begin{pmatrix} \alpha_{11} & \alpha_{12} & \cdots & \alpha_{1n} \\ \alpha_{21} & \alpha_{22} & \cdots & \alpha_{2n} \\ \vdots & \vdots & & \vdots \\ \alpha_{m1} & \alpha_{m2} & \cdots & \alpha_{mn} \end{pmatrix}, \text{ 那末 } {}^tF = \begin{pmatrix} \alpha_{11} & \alpha_{21} & \cdots & \alpha_{m1} \\ \alpha_{12} & \alpha_{22} & \cdots & \alpha_{m2} \\ \vdots & \vdots & & \vdots \\ \alpha_{1n} & \alpha_{2n} & \cdots & \alpha_{mn} \end{pmatrix}.$$

**証明** 假定  $V_1 = [a_1, a_2, \dots, a_n]$ ,  $V_2 = [b_1, b_2, \dots, b_m]$ ,

$$\hat{V}_1 = [\hat{a}_1, \hat{a}_2, \dots, \hat{a}_n], \hat{V}_2 = [\hat{b}_1, \hat{b}_2, \dots, \hat{b}_m].$$

由  $F = (\alpha_{ik})$  得  $f(a_k) = \alpha_{1k}b_1 + \cdots + \alpha_{mk}b_m$  ( $k=1, 2, \dots, n$ ).

要証明  ${}^tF = (\alpha_{ki})$ , 只要証明  ${}^tf(\hat{b}_i) = \alpha_{i1}\hat{a}_1 + \cdots + \alpha_{in}\hat{a}_n$  ( $i=1, 2, \dots, m$ ) 即可。但是在这里只要示明对于任意  $k$  ( $k=1, 2, \dots, n$ ),  ${}^tf(\hat{b}_i)(a_k) = (\alpha_{i1}\hat{a}_1 + \cdots + \alpha_{in}\hat{a}_n)(a_k)$  成立就行了。因为  $(\alpha_{i1}\hat{a}_1 + \cdots + \alpha_{in}\hat{a}_n)(a_k) = \alpha_{ik}$ ,  ${}^tf(\hat{b}_i)(a_k) = \hat{b}_i \cdot f(a_k) = \hat{b}_i(\alpha_{1k}b_1 + \cdots + \alpha_{mk}b_m) = \alpha_{ik}$ , 所以它成立。

**例 3** §8 例 6 中的  $F(v_1, v_2, \dots, v_n)$ ,  $Q(v_1, v_2, \dots, v_n)$  是互为轉置矩陣。

**命題 20**  ${}^t(f_1 + f_2) = {}^tf_1 + {}^tf_2$ ,  ${}^t(\lambda f) = \lambda {}^tf$ ,  ${}^t(g \circ f) = {}^tf \circ {}^tg$ ,

$${}^t(F_1 \div F_2) = {}^tF_1 \div {}^tF_2, {}^t(\lambda F) = \lambda {}^tF, {}^t(GF) = {}^tF {}^tG.$$

**証明** 只須証明  ${}^t(g \circ f) = {}^tf \circ {}^tg$ .  $V_1 \xrightarrow{f} V_2 \xrightarrow{g} V_3 \xrightarrow{\xi} K$  其余都是明显的。

对于任意  $\xi \in \hat{V}$ ,

$$\begin{aligned} {}^t(g \circ f)(\xi) &= \xi \circ (g \circ f) \\ &= (\xi \circ g) \circ f = ({}^tg(\xi)) \circ f = {}^tf({}^tg(\xi)) \\ &= ({}^tf \circ {}^tg)(\xi). \end{aligned}$$

所以

$${}^t(g \circ f) = {}^tf \circ {}^tg.$$

**定理 11**  $r(f) = r({}^tf)$ .

**証明** 假設  $\dim V_1 = n$ ,  $\dim V_2 = m$ ,  $r(f) = \dim \operatorname{Im} f = r$ . 如果  $(\operatorname{Im} f)'$  是  $\operatorname{Im} f$  的零化空間, 那末  $(\operatorname{Im} f)' \subset \hat{V}_2$ ,  $\dim(\operatorname{Im} f)'$

$= m - r$ . 但是

$$\begin{aligned}\xi \in (\operatorname{Im} f)' &\Leftrightarrow \xi(\operatorname{Im} f) = 0 \Leftrightarrow \xi \cdot f(V_1) = 0 \\ &\Leftrightarrow ({}^t f(\xi))(V_1) = 0 \Leftrightarrow {}^t f(\xi) = 0 \\ &\Leftrightarrow \xi \in \operatorname{Ker} {}^t f,\end{aligned}$$

因此

$$\operatorname{Ker} {}^t f = (\operatorname{Im} f)',$$

所以  $r({}^t f) = m - \dim(\operatorname{Ker} {}^t f) = m - \dim(\operatorname{Im} f)' = r$ .

**系 1** 假定  $F$  是任意矩阵, 那末  $r(F) = r({}^t F)$ .

**系 2**  $r(F)$  也等于  $F$  的行向量中无关的个数。

**系 3** 矩阵的列向量中无关的个数与行向量中无关的个数相等。

在矩阵  $F$  中把除去它的若干行及若干列所成的矩阵作为是  $G$ , 表为  $F \supset G$ . 假如

$$F = \begin{pmatrix} \alpha_{11} & \alpha_{12} & \cdots & \alpha_{1n} \\ \alpha_{21} & \alpha_{22} & \cdots & \alpha_{2n} \\ \vdots & \vdots & & \vdots \\ \alpha_{m1} & \alpha_{m2} & \cdots & \alpha_{mn} \end{pmatrix},$$

那末 
$$G = \begin{pmatrix} \alpha_{r_1 \mu_1} & \alpha_{r_1 \mu_2} & \cdots & \alpha_{r_1 \mu_k} \\ \alpha_{r_2 \mu_1} & \alpha_{r_2 \mu_2} & \cdots & \alpha_{r_2 \mu_k} \\ \vdots & \vdots & & \vdots \\ \alpha_{r_l \mu_1} & \alpha_{r_l \mu_2} & \cdots & \alpha_{r_l \mu_k} \end{pmatrix}, \quad \begin{pmatrix} k \leq n \\ l \leq m \end{pmatrix}.$$

**系 4** 假定  $F \supset G$ , 那末  $r(F) \geq r(G)$ .

**证明** 假定除去矩阵  $F$  中若干列所成的矩阵是  $F'$ , 那末  $F'$  的列向量中无关的个数不超过  $F$  的列向量中无关的个数, 因而  $r(F) \geq r(F')$ . 再假定除去  $F'$  中若干行所成的矩阵是  $F''$ , 比较  $F'$  与  $F''$  的行向量中无关的个数, 即得  $r(F') \geq r(F'')$ , 于是  $r(F) \geq r(F'')$ .

因为  $G$  能够象这样由  $F$  来形成, 所以  $r(F) \geq r(G)$ . (证毕)

**定理 12** 假定  $F$  是任意矩阵, 那末存在象

$$F \supset F_{00}$$

这样的正則矩陣  $F_{00}$ .

这  $F_{00}$  叫做  $F$  的**主部**。

**証明** 假定  $r(F) = r$ , 那末  $F$  的列向量中无关的恰好有  $r$  个, 只把它們留下而将其余各列都除去所成的矩陣假定是  $F_0$ , 那末  $r(F_0) = r$ . 又因为  $F_0$  的行向量中无关的恰好有  $r$  个, 所以只留下它們而将其余各行都除去所成的矩陣假定是  $F_{00}$ , 那末  $r(F_{00}) = r$ . 显然  $F_{00}$  是  $r$  級方陣, 所以  $F_{00}$  是正則的。 (証毕)

由 § 8 例 6, 对于  $F$  用适当的正則矩陣左及右相乘就能够使主部在“左上”位置。

## § 11 1 次 方 程

1 次方程的原型, 中学以来就知道的, 是

$$ax = b \quad (11.1)$$

形状的方程。在中学所討論的一般是在  $a, b \in \mathbf{R}$  情况下, 求滿足 (11.1) 的  $x \in \mathbf{R}$ . 因为以任意体  $K$  代替  $\mathbf{R}$  来考虑时, 理論完全相同, 所以以下假定  $a, b, x \in K$  ( $K$  是任意体)。如所周知, (11.1) 的解

(i) 假如  $a \neq 0$ , 那末  $x = \frac{b}{a}$ .

(ii) 假如  $a = 0, b = 0$ , 那末  $x$  是  $K$  中任意元。

(iii) 假如  $a = 0, b \neq 0$ , 那末不論  $x$  取任何值, (11.1) 不成立。

(i) 的情况, 解是唯一的。它叫做**正則情况**。又 (ii) 叫做**不定情况**, 而 (iii) 叫做**不能情况**。假如 (11.1) 的解的集合是  $S$ , 那末对于 (i), (ii), (iii) 各种情况, 分别是  $S = \{b/a\}$ ,  $S = K$ ,  $S = \emptyset$ .

假定  $f(x) = ax$ , 把  $f$  看成自  $K^1$  到  $K^1$  的綫性映射, 因此  $S = f^{-1}(b)$ . 一般, 給定了自  $K$  上向量空間  $V_1$  到  $V_2$  的綫性映射  $f$  与  $y \in V_2$  时, 把求滿足  $f(x) = y$  的  $x$  的集合  $f^{-1}(y)$  叫做解 **1 次方程**

$$f(x) = y, \quad (11.2)$$

(“1 次”是“綫性”的同义語之一, 在上面已叙述过。) 当  $f_1, f_2 \in \mathfrak{L}(V_1, V_2)$ ,  $y_1, y_2 \in V_2$  时, 假如  $f_1^{-1}(y_1) = f_2^{-1}(y_2)$ , 那末两个 1 次方程  $f_1(x) = y_1, f_2(x) = y_2$  叫做**等价**。

**命题 21** 当  $f^{-1}(y) \neq \emptyset$  时, 假如  $x_0 \in f^{-1}(y)$ , 那末  $f^{-1}(y) = (x_0 + u; u \in \text{Ker } f)$ . (这右边用  $x_0 + \text{Ker } f$  表示。)

**証明** 由  $x \in f^{-1}(y) \Leftrightarrow f(x) = y \Leftrightarrow f(x - x_0) = f(x) - f(x_0) = 0 \Leftrightarrow x - x_0 \in \text{Ker } f$ , 自明。 (証毕)

当  $f^{-1}(y) = \emptyset$  时, 1 次方程 (11.2) 叫做**不能**,  $f^{-1}(y)$  只由一个元构成时, (11.2) 叫做**正則**。不是不能也不是正則时, (11.2) 叫做**不定**。在不定情况,  $f^{-1}(y)$  中任意一元  $x_0$  叫做 (11.2) 的**特殊解**,  $x_0 + \text{Ker } f$  叫做 (11.2) 的**一般解**。因此求一般解的問題归結于求特殊解及求  $\text{Ker } f$ 。

**例 1** 假定  $f$  是全单射, 那末 (11.2) 总是正則。假如  $f$  是单射,  $y \in \text{Im } f$ , 那末 (11.2) 正則。  $y \notin \text{Im } f$  与 (11.2) 不能等价。

在 (11.2) 中,  $y = 0$  时, (11.2) 叫做**齐次方程**,  $y \neq 0$  时, (11.2) 叫做**非齐次方程**。(11.2) 是非齐次方程时, 左边用 0 代替所得的

$$f(x) = 0$$

叫做**同伴**于 (11.2) 的齐次方程。解它不外是求  $\text{Ker } f$ 。

**例 2** 解綫性微分方程

$$\frac{d^n y}{dx^n} + p_1(x) \frac{d^{n-1} y}{dx^{n-1}} + \cdots + p_{n-1}(x) \frac{dy}{dx} = p(x) \quad (1)$$

( $p_1(x), \cdots, p_{n-1}(x), p(x)$  都是連續函数)

时, 假如命

$$\Delta = D^n + p_1 D^{n-1} + \cdots + p_{n-1} D \in \mathfrak{L}(\mathbb{C}^n, {}^0\mathbb{C}) \quad (\S 7 \text{ 例 } 7),$$

就不外是解 1 次方程

$$\Delta(f) = p,$$

因此用 (1) 的一个特殊解  $f_0(x)$  及同伴齐次方程

$$\frac{d^n y}{dx^n} + p_1(x) \frac{d^{n-1} y}{dx^{n-1}} + \cdots + p_{n-1}(x) \frac{dy}{dx} = 0$$





$$r(F) = r(F_1) \Leftrightarrow y \in [a_1, a_2, \dots, a_n]$$

$$\Leftrightarrow y = \xi_1 a_1 + \xi_2 a_2 + \dots + \xi_n a_n, \xi_i \in K.$$

这最后一式就与 (11.3') 有解  $\begin{pmatrix} \xi_1 \\ \xi_2 \\ \vdots \\ \xi_n \end{pmatrix}$  等价。

**命题 23** 假定  $F$  是正则矩阵, 那末方程 (11.3) 或 (11.3') 也是正则, 它的解是  $x = F^{-1}y$ .

**证明** 假定  $F$  是正则的, 引用  $F^{-1}$  得

$$Fx = y \Leftrightarrow F^{-1}Fx = F^{-1}y \Leftrightarrow x = F^{-1}y.$$

所以 (11.3) 或 (11.3') 只有一个解  $x = F^{-1}y$ . 因此是正则。

**命题 24** (11.3) 是正则的必要充分条件是 (11.3) 不是不能并且  $r(F) = n$ .

**证明** 当 (11.3) 不是不能时, 它的解可表为  $x_0 + \text{Ker } F$ , 所以 (11.3) 是正则  $\Leftrightarrow \text{Ker } F = \{0\} \Leftrightarrow r(F) = n - \dim \text{Ker } F = n$ .

**系** 假定 (11.3) 不是不能并且  $m < n$ , 那末 (11.3) 是不定的.

**证明** 因为  $r(F) \leq \min(m, n)$ , 所以  $r(F) \leq m < n$ . 于是由命题 24, (11.3) 不是正则的. (证毕)

假如互换矩阵  $F$  的  $m$  个行, 对于  $\eta_1, \eta_2, \dots, \eta_m$  也施行与它相同的互换, 那末在 (11.3) 中只是改变方程的顺序, 显然得到与它等价的方程。再互换  $F$  的  $n$  个列, 只是改变“未知数的名称”。能够得到在本质上仍然与它相同的方程。因此不失一般性,  $F$  的主部可假定在左上位置。

**命题 25** 假定方程 (11.3) 不是不能,  $r(F) = r$ , 并且  $F$  的主部在左上位置, 那末 (11.3) 与它最初的  $r$  个方程等价。

**证明** 假定  $F$  的各个行向量是  ${}_1b, {}_2b, \dots, {}_mb$ , 那末 (11.3) 中各式成为

$${}_1bx = \eta_1, {}_2bx = \eta_2, \dots, {}_mbx = \eta_m. \quad (11.3'')$$

因为  $\{_1b, _2b, \dots, _mb\}$  中最初  $r$  个綫性无关, 所以

$$_ib = \lambda_1^{(i)} \cdot _1b + \lambda_2^{(i)} \cdot _2b + \dots + \lambda_r^{(i)} \cdot _rb \quad (i = r+1, r+2, \dots, m),$$

因此 (11.3'') 中前  $r$  个方程如果成立, 則剩下的  $(m-r)$  个也必然成立。所以 (11.3) 与它最初的  $r$  个方程等价。 (証毕)

由命题 25, 对于 (11.3) 可假定  $m = r(F)$  不失一般性。

**定理 13** 假定在 (11.3),  $m = r(F)$  并且  $F$  的主部  $F_0$  在左上位置,  $F = (F_0 F_*)$ ,  $F_0 \in \mathfrak{M}(m, K)$ ,  $F_* \in \mathfrak{M}(m, n-m; K)$ , 那末 (11.3) 的一个解为

$$x_0 = \begin{pmatrix} F_0^{-1}y \\ O_{n-m, 1} \end{pmatrix}.$$

如果  $n = m$ , 則方程成为正則 (因而它沒有其他解)。如果  $n - m = s > 0$ , 那末 (11.3) 成为不定,  $\begin{pmatrix} F_0^{-1}F_* \\ -E_s \end{pmatrix}$  中  $s$  个列向量形成  $\text{Ker } F$  的基底。

**証明** 因为  $Fx_0 = F \begin{pmatrix} F_0^{-1}y \\ O \end{pmatrix} = (F_0 F_*) \begin{pmatrix} F_0^{-1}y \\ O \end{pmatrix} = (F_0 F_0^{-1}y + O) = y$ , 所以  $x_0$  是 (11.3) 的一个解。

因为  $\dim \text{Ker } F = n - r(F) = n - m$ , 假如  $m = n$ , 那末  $\text{Ker } F = \{0\}$ . 所以方程 (11.3) 成为正則。

假如  $n - m = s > 0$ , 那末  $\dim \text{Ker } F = s$ . 因此假如  $\begin{pmatrix} F_0^{-1}F_* \\ -E_s \end{pmatrix}$  的  $s$  个列向量是  $a_1, a_2, \dots, a_s$ , 如果能够証明它們都  $\in \text{Ker } F$ , 并且  $\{a_1, a_2, \dots, a_s\}$  綫性无关, 那末它們显然成为  $\text{Ker } F$  的基底。

$$\begin{aligned} F \begin{pmatrix} F_0^{-1}F_* \\ -E_s \end{pmatrix} &= \underset{\substack{\xrightarrow{m} \\ \xleftarrow{s}}}{(F_0 F_*)} \begin{pmatrix} F_0^{-1}F_* \\ -E_s \end{pmatrix} \underset{\substack{\uparrow m \\ \downarrow s}}{=} \\ &= (F_0 F_0^{-1}F_* - F_* E_s) = O_{m, s}, \end{aligned}$$

这表示  $Fa_i = 0$  ( $i = 1, 2, \dots, s$ ). 所以  $a_i \in F^{-1}(0)$  ( $i = 1, 2, \dots, s$ ).

又假如  $\lambda_1 a_1 + \lambda_2 a_2 + \dots + \lambda_s a_s = 0$ , 如果着眼于第  $(m+i)$  行元素就得到  $-\lambda_i = 0$  ( $i = 1, 2, \dots, s$ ), 所以  $\{a_1, a_2, \dots, a_s\}$  綫性无关。

## § 12 行 列 式

方程 (11.3) 的实际解法有在中学里所熟知的消去法, 及其他种种。在这里我们叙述用行列式的解法 (关于各种实际解法参照古屋茂氏: 矩阵与行列式)。

由前节的结果, 1 次方程

$$Fx = y \quad (12.1)$$

的解法归结于解下面关于已知方阵  $F_0$  的两个问题:

- (i) 判定  $F_0$  是否正则,
- (ii) 当  $F_0$  是正则时, 计算  $F_0^{-1}$ .

实际上, 假如 (i), (ii) 能够解决, 那末方程 (12.1) 可以按照下面的顺序来求解。

首先来考查是否  $r(F) = r(F_1)$ , 因为  $r(F)$  是含于  $F$  中的最大正则矩阵的级数, 所以假如在含于  $F$  的方阵中,  $r$  级的正则矩阵至少有一存在, 而  $(r+1)$  级以上的方阵都不正则, 那末  $r(F) = r$ , 同样可以求出  $r(F_1)$ . 如果  $r(F) \neq r(F_1)$ , 那末方程是不能。

当  $r(F) = r(F_1)$  时, 设含于  $F$  的  $r$  级正则矩阵 ( $F$  的主部) 之一假定是  $F_0$ . 适当改变方程的顺序及未知数的名称, 可以使得  $F_0$  在左上位置。这时最初的  $r$  个方程如果是  $(F_0 F_*)x = y$ , 那末解它即可。

假如未知数的个数即  $x$  的维数也等于  $r$ , 那末方程成为  $F_0 x = y$ . 它是正则方程, 解由  $x = F_0^{-1}y$  给出。

当未知数的个数比  $r$  大时, 由定理 13, 一个特殊解用  $x_0 = \begin{pmatrix} F_0^{-1}y \\ 0_{n-r,1} \end{pmatrix}$  给出。同伴齐次方程的一般解当  $\begin{pmatrix} F_0^{-1}F_* \\ -E_{n-r} \end{pmatrix}$  的列向量假定是  $a_1, a_2, \dots, a_{n-r}$  时, 用  $\sum_{i=1}^{n-r} \lambda_i a_i$  给出, 所以 (12.1) 的一般解是

$$x = \begin{pmatrix} F_0^{-1}y \\ O_{n-r,1} \end{pmatrix} + \sum_{i=1}^{n-r} \lambda_i a_i.$$

上面两个问题 (i), (ii) 可以用行列式来解答。首先来叙述行列式的定义。

行列式  $D_n$  是自  $\mathfrak{M}(n, K)$  到  $K$  的映射, 关于  $n$  归纳定义如下:

(i) 假如  $n=1$ , 那末  $\mathfrak{M}(1, K) = K$ , 这时  $D_1 = e_K$  ( $K$  的恒等映射)。

(ii) 当  $n > 1$  时, 设自  $F \in \mathfrak{M}(n, K)$  除去第一行  $(\alpha_{11}, \dots, \alpha_{1n})$  所得的  $(n-1, n)$  型矩阵是  $F^*$ , 自  $F^*$  除去第  $i$  列所得的  $(n-1, n-1)$  型矩阵假定是  $F_i^*$ . 假如  $D_{n-1}$  已定义, 这时

$$D_n(F) = \sum_{i=1}^n (-1)^{1+i} \alpha_{1i} D_{n-1}(F_i^*).$$

$D_n(F)$  叫做  $F$  的行列式, 用  $|F|$  或  $\det F$  表示。显然  $D_n(F)$  能够对于  $F$  中各元素施行加减乘法而求得。

**例 1**  $D_1(\alpha) = \alpha \textcircled{1}$ ,

$$\begin{aligned} \begin{vmatrix} \alpha_{11} & \alpha_{12} \\ \alpha_{21} & \alpha_{22} \end{vmatrix} &= \alpha_{11}\alpha_{22} - \alpha_{12}\alpha_{21}, \\ \begin{vmatrix} \alpha_{11} & \alpha_{12} & \alpha_{13} \\ \alpha_{21} & \alpha_{22} & \alpha_{23} \\ \alpha_{31} & \alpha_{32} & \alpha_{33} \end{vmatrix} &= \alpha_{11} \begin{vmatrix} \alpha_{22} & \alpha_{23} \\ \alpha_{32} & \alpha_{33} \end{vmatrix} - \alpha_{12} \begin{vmatrix} \alpha_{21} & \alpha_{23} \\ \alpha_{31} & \alpha_{33} \end{vmatrix} + \alpha_{13} \begin{vmatrix} \alpha_{21} & \alpha_{22} \\ \alpha_{31} & \alpha_{32} \end{vmatrix} \\ &= \alpha_{11}(\alpha_{22}\alpha_{33} - \alpha_{23}\alpha_{32}) - \alpha_{12}(\alpha_{21}\alpha_{33} - \alpha_{23}\alpha_{31}) \\ &\quad + \alpha_{13}(\alpha_{21}\alpha_{32} - \alpha_{22}\alpha_{31}) \\ &= \alpha_{11}\alpha_{22}\alpha_{33} + \alpha_{12}\alpha_{23}\alpha_{31} + \alpha_{13}\alpha_{32}\alpha_{21} - \alpha_{31}\alpha_{22}\alpha_{13} \\ &\quad - \alpha_{32}\alpha_{23}\alpha_{11} - \alpha_{33}\alpha_{21}\alpha_{12}. \end{aligned}$$

**例 2**  $\begin{vmatrix} \alpha_{11} & 0 & 0 & \cdots & 0 \\ 0 & \alpha_{22} & 0 & \cdots & 0 \\ 0 & 0 & \alpha_{33} & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & \alpha_{nn} \end{vmatrix} = \alpha_{11}\alpha_{22}\cdots\alpha_{nn} \quad (\text{对角线型}).$

**①**  $n=1$  时, 与  $D_1(\alpha) = |\alpha|$  不太通行, 因为恐怕与  $\alpha$  的绝对值混淆。

一般,

$$\begin{vmatrix} \alpha_{11} & 0 & 0 & \cdots & 0 \\ \alpha_{21} & \alpha_{22} & 0 & \cdots & 0 \\ \alpha_{31} & \alpha_{32} & \alpha_{33} & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ \alpha_{n1} & \alpha_{n2} & \alpha_{n3} & \cdots & \alpha_{nn} \end{vmatrix} = \alpha_{11}\alpha_{22}\cdots\alpha_{nn} \quad (\text{第1三角型}).$$

假如把矩阵  $F$  的第  $i$  行写成  $i b$ , 第  $k$  列写成  $a_k$ , 那末

$$D_n(F) = D_n(a_1 \ a_2 \ \cdots \ a_n) = D_n \begin{pmatrix} {}_1b \\ {}_2b \\ \vdots \\ {}_nb \end{pmatrix}$$

可以看成  $n$  个向量  $a_k$  或  $n$  个向量  $i b$  的函数。在这里固定  $a_2, a_3, \cdots, a_n$  而考虑  $D_n(F)$  只是  $a_1$  的函数时, 把  $D_n(F)$  写成  $D_n^1(a_1)$ . 同样定义  $D_n^k(a_k)$ ,  ${}^i D_n(i b)$ .

**命题 26** (i)  $D_n^k \in \mathfrak{Q}(K^n, K)$ , (ii)  ${}^i D_n \in \mathfrak{Q}({}^n K, K)$ .

**证明** 关于  $n$  用归纳法。

(i) 当  $n=1$  时,  $D_1^1 = D_1 = e_K \in \mathfrak{Q}(K^1, K)$ .

$$F = \left( \begin{array}{c|c} \alpha_{11} & \alpha_{12} \cdots \alpha_{1n} \\ \hline a_1^* & F_1^* \end{array} \right).$$

当  $n > 1$  时, 假定  $D_{n-1}^k \in \mathfrak{Q}(K^{n-1}, K)$  已证明。命  $a_1 = \begin{pmatrix} \alpha_{11} \\ a_1^* \end{pmatrix}$ ,

那末

$$\begin{aligned} D_n^1(a_1) &= D_n(F) = \alpha_{11} D_{n-1}(F_1^*) + \sum_{i=2}^n (-1)^{1+i} \alpha_{1i} D_{n-1}(F_i^*) \\ &= \alpha_{11} D_{n-1}(F_1^*) + \sum_{i=2}^n (-1)^{1+i} \alpha_{1i} D_{n-1}^1(a_1^*), \end{aligned}$$

因为  $D_{n-1}^1 \in \mathfrak{Q}(K^{n-1}, K)$ , 所以

$$\begin{aligned} D_n^1(a_1 + a_1') &= (\alpha_{11} + \alpha'_{11}) D_{n-1}(F_1^*) \\ &\quad + \sum_{i=2}^n (-1)^{1+i} \alpha_{1i} (D_{n-1}^1(a_1^*) + D_{n-1}^1(a_1'^*)) \end{aligned}$$

$$= D_n^1(a_1) + D_n^1(a'_1) \textcircled{1}.$$

同样  $D_n^1(\lambda a_1) = \lambda D_n^1(a_1).$

所以  $D_n^1 \in \mathfrak{L}(K^n, K).$

同样  $D_n^k \in \mathfrak{L}(K^n, K).$

(ii) 当  $n=1$  时,  ${}^1D_1 = D_1 = e_K \in \mathfrak{L}({}^1K, K).$

当  $n>1$  时,  ${}^1D_n \in \mathfrak{L}({}^nK, K)$  由  $D_n$  的定义自明 $\textcircled{2}$ 。一般, 假定  ${}^{i-1}D_{n-1} \in \mathfrak{L}({}^{n-1}K, K)$ ,  $F_i^*$  的第  $(i-1)$  行为  ${}^{i-1}b^{(i)}$ , 那末

$${}^iD_n({}^ib) = \sum_{j=1}^n (-1)^{1+j} \alpha_{1j} {}^{i-1}D_{n-1}({}^{i-1}b^{(j)}).$$

但是由归纳法的假定,  ${}^{i-1}D_{n-1} \in \mathfrak{L}({}^{n-1}K, K)$ , 所以

$${}^iD_n({}^ib) \in \mathfrak{L}({}^nK, K).$$

**命题 27** 当  $n \geq 2$  时,

(i) 两列是相同向量的矩阵的行列式等于 0, 即假如  $a_k = a_{k'} (k \neq k')$ , 那末  $D_n(F) = 0$ .

(ii) 假如把  $(a_1 \cdots a_i \cdots a_k \cdots a_n)$  中两列  $a_i, a_k$  互换所成的矩阵是  $(a_1 \cdots a_k \cdots a_i \cdots a_n)$ , 那末  $D(a_1 \cdots a_i \cdots a_k \cdots a_n) = -D(a_1 \cdots a_k \cdots a_i \cdots a_n)$ .

**证明** 关于  $n$  用归纳法, 当  $n=2$  时, 引用例 1 的结果立即明白。对于  $n-1$ , 假定 (i), (ii) 成立。在  $F$  中当  $a_k = a_{k'}$  时,

$$D_n(F) = \alpha_{1k} D_{n-1}(F_k^*) + \alpha_{1k'} D_{n-1}(F_{k'}^*) + \sum_{i \neq k, k'} \alpha_{1i} D_{n-1}(F_i^*),$$

前两项的和根据  $\alpha_{1k} = \alpha_{1k'}$ ,  $D_{n-1}(F_k^*) = -D_{n-1}(F_{k'}^*)$  (归纳法假定) 是 0。在剩下的项中,  $F_i^*$  含两列相同的向量, 又由归纳法假定各项都成为 0。因此 (i) 成立。

$\textcircled{1}$  因为  $D'_{n-1} \in \mathfrak{L}(K^{n-1}, K)$ , 所以  $D'_{n-1}(a_1^* + a_1'^*) = D'_{n-1}(a_1^*) + D'_{n-1}(a_1'^*)$ . ——译者注

$\textcircled{2}$  因为  ${}^1D_n({}^1a + {}^1a') = \sum (-1)^{1+i} (\alpha_{1i} + \alpha'_{1i}) D_{n-1}(F_i^*) = \sum_{i=1}^n (-1)^{1+i} \alpha_{1i} D_{n-1}(F_i^*) + \sum_{i=1}^n (-1)^{1+i} \alpha'_{1i} D_{n-1}(F_i^*) = {}^1D_n({}^1a) + {}^1D_n({}^1a')$ , 所以  ${}^1D_n \in \mathfrak{L}({}^nK, K)$ . ——译者注

再由命题 26(i),

$$\begin{aligned} 0 &= D_n(a_1 + a_2 \quad a_1 + a_2 \quad a_3 \cdots a_n) \\ &= D_n(a_1 \quad a_2 \quad a_3 \cdots a_n) + D_n(a_1 \quad a_2 \quad a_3 \cdots a_n) \\ &\quad + D_n(a_2 a_1 a_3 \cdots a_n) + D_n(a_2 a_2 a_3 \cdots a_n) \\ &= D_n(a_1 a_2 a_3 \cdots a_n) + D_n(a_2 a_1 a_3 \cdots a_n). \end{aligned}$$

所以

$$D_n(a_1 a_2 a_3 \cdots a_n) = -D_n(a_2 a_1 a_3 \cdots a_n).$$

同样  $D_n(a_1 \cdots a_i \cdots a_k \cdots a_n) = -D_n(a_1 \cdots a_k \cdots a_i \cdots a_n)$ .

**系 1** 假如  $F$  中列向量  $a_1, a_2, \dots, a_n$  线性相关, 那末  $D_n(F) = 0$ .

**证明** 当  $n=1$  时,  $F = (0)$ , 所以  $D_1(0) = 0$ .

当  $n \geq 2$  时, 譬如  $a_1 = \sum_{i=2}^n \lambda_i a_i$  ( $\lambda_i \in K$ ), 引用命题 26(i) 得

$$D_n(F) = D_n\left(\sum_{i=2}^n \lambda_i a_i, a_2, \dots, a_n\right) = \sum_{i=2}^n \lambda_i (a_i \cdots a_i \cdots a_n) = 0.$$

**系 2** 假如  $r(F) < n$ , 那末  $D_n(F) = 0$ .

**证明** 假如  $r(F) < n$ , 那末  $F$  的列向量  $a_1, a_2, \dots, a_n$  线性相关, 因此由系 1 自明。

**注意** 由命题 27 已导出系 1, 系 2. 反之由系 2 也能导出命题 27, 即假定系 2 成立, 那末命题 27(i) 显然成立, 因而(ii)也成立<sup>①</sup>.

把  $E_n$  作为例 2 中对角线型矩阵的特殊情况来考虑, 可直接得到下面的命题。

**命题 28**  $D_n(E_n) = 1$ .

假定  $(\nu_1, \nu_2, \dots, \nu_n)$  是  $(1, 2, \dots, n)$  的任意排列, 自  $(\nu_1, \nu_2, \dots, \nu_n)$  中任意取出两数  $(\nu_i, \nu_j)$ , 如果左边的数大于右边的数, 那

<sup>①</sup> 因为  $D_n^k \in \mathcal{L}(K^n, K)$ , 所以  $D_n(a_1 \cdots a_i + a_k \cdots a_k + a_i \cdots a_n) = D_n(a_1 \cdots a_i \cdots a_k \cdots a_n) + D_n(a_1 \cdots a_k \cdots a_i \cdots a_n) = 0$ . 因此  $D_n(a_1 \cdots a_i \cdots a_k \cdots a_n) = -D_n(a_1 \cdots a_k \cdots a_i \cdots a_n)$ .  
——译者注



末在此处就說有一反序。含于  $(\nu_1, \nu_2, \dots, \nu_n)$  的反序总数假如是  $I$ , 規定  $\text{sgn}(\nu_1, \nu_2, \dots, \nu_n) = (-1)^I$ . 按照  $\text{sgn}(\nu_1, \nu_2, \dots, \nu_n) = 1$  及  $-1$ , 分別把  $(\nu_1, \nu_2, \dots, \nu_n)$  叫做偶排列, 奇排列。計算  $I$  的实际方法, 可以象下面那样来进行。在  $(\nu_1, \nu_2, \dots, \nu_n)$  中, 在 1 左边的数的个数假如是  $I_1$ , 一般在  $k$  左边比  $k$  大的数的个数假如是  $I_k$ , 那末  $\sum_{k=1}^{n-1} I_k = I$ .

在排列  $(\nu_1, \nu_2, \dots, \nu_n)$  中, 先把 1 与在它左边的数作  $I_1$  回互換, 那末 1 就在最左边。次把 2 与在它左边的作  $I_2$  回互換, 2 就在 1 的后面。余类推。在  $(\nu_1, \nu_2, \dots, \nu_n)$  中总共施行  $I$  回“两数字的互換”(对換)就能够使它成为正常排列  $(1, 2, \dots, n)$ .

**系 1** 用 § 8 例 6 的記法, 假如  $Q(\nu_1, \nu_2, \dots, \nu_n) = (e_{\nu_1} e_{\nu_2} \dots e_{\nu_n})$ , 那末  $D_n(Q(\nu_1, \nu_2, \dots, \nu_n)) = \text{sgn}(\nu_1, \nu_2, \dots, \nu_n)$ .

**証明** 对于  $Q(\nu_1, \nu_2, \dots, \nu_n) = (e_{\nu_1} e_{\nu_2} \dots e_{\nu_n})$  的列施行  $I$  回对換能够把这矩陣变为  $(e_1 e_2 \dots e_n) = E_n$ . 由命題 27, 对于各个对換行列式只改变符号, 所以  $D_n(Q(\nu_1, \nu_2, \dots, \nu_n)) = (-1)^I D_n(E_n) = \text{sgn}(\nu_1, \nu_2, \dots, \nu_n)$ .

**系 2** 自  $F$  中各列各行各取出一元素  $\alpha_{\nu_1, 1}, \alpha_{\nu_2, 2}, \dots, \alpha_{\nu_n, n}$ , 作  $\text{sgn}(\nu_1, \nu_2, \dots, \nu_n) \alpha_{\nu_1, 1} \alpha_{\nu_2, 2} \dots \alpha_{\nu_n, n}$ , 那末  $D_n(F)$  等于这样的  $n!$  个积的总和, 即

$$D_n(F) = \sum \text{sgn}(\nu_1, \nu_2, \dots, \nu_n) \alpha_{\nu_1, 1} \alpha_{\nu_2, 2} \dots \alpha_{\nu_n, n}.$$

$$\text{証明 } F = \left( \sum_{\nu_1=1}^n \alpha_{\nu_1, 1} e_{\nu_1} \sum_{\nu_2=1}^n \alpha_{\nu_2, 2} e_{\nu_2} \dots \sum_{\nu_n=1}^n \alpha_{\nu_n, n} e_{\nu_n} \right).$$

所以由命題 27(i),

$$\begin{aligned} D_n(F) &= \sum D_n(\alpha_{\nu_1, 1} e_{\nu_1} \alpha_{\nu_2, 2} e_{\nu_2} \dots \alpha_{\nu_n, n} e_{\nu_n}) \\ &= \sum D_n(e_{\nu_1} e_{\nu_2} \dots e_{\nu_n}) \alpha_{\nu_1, 1} \alpha_{\nu_2, 2} \dots \alpha_{\nu_n, n}. \end{aligned}$$

这里  $\Sigma$  是  $n^n$  个行列式的綫性組合, 但因为其中在  $\nu_1, \nu_2, \dots, \nu_n$  中有相等的項都成为 0, 所以就成为象下面那样  $n!$  个項的和

$$\begin{aligned} D_n(F) &= \sum D_n(Q(\nu_1, \nu_2, \dots, \nu_n)) \alpha_{\nu_1 1} \alpha_{\nu_2 2} \cdots \alpha_{\nu_n n} \\ &= \sum \operatorname{sgn}(\nu_1, \nu_2, \dots, \nu_n) \alpha_{\nu_1 1} \alpha_{\nu_2 2} \cdots \alpha_{\nu_n n}. \quad (\text{証毕}) \end{aligned}$$

**命题 29** 假定  $\mathfrak{D}_n: \mathfrak{M}(n, K) \rightarrow K$ , 并且满足下列两条件:

(i) 如果把  $\mathfrak{D}_n$  看成第  $k$  列的函数, 写成  $\mathfrak{D}_n^k$ , 那末

$$\mathfrak{D}_n^k \in \mathfrak{L}(K^n, K) \quad (k=1, 2, \dots, n),$$

(ii) 如果  $r(F) < n$ , 那末  $\mathfrak{D}_n(F) = 0$ ,

则

$$\mathfrak{D}_n(F) = D_n(F) \mathfrak{D}_n(E_n).$$

**证明** 可以与命题 28 系 2 完全一样, 象下面那样导出

$$\begin{aligned} \mathfrak{D}_n(F) &= \mathfrak{D}_n(a_1 \cdots a_n) = \mathfrak{D}_n(\sum \alpha_{\nu_1 1} e_{\nu_1} \cdots \sum \alpha_{\nu_n n} e_{\nu_n}) \\ &= \sum \alpha_{\nu_1 1} \cdots \alpha_{\nu_n n} \mathfrak{D}_n(e_{\nu_1} \cdots e_{\nu_n}) \\ &= \sum \alpha_{\nu_1 1} \cdots \alpha_{\nu_n n} \operatorname{sgn}(\nu_1, \dots, \nu_n) \mathfrak{D}_n(E_n) \\ &= D_n(F) \mathfrak{D}_n(E_n). \end{aligned}$$

**例 3**  $\begin{vmatrix} A_r & O_{r,s} \\ O_{s,r} & B_s \end{vmatrix} = |A_r| \cdot |B_s|,$

[解] 固定  $B_s$ , 把  $D_r = \begin{vmatrix} A_r & O \\ O & B_s \end{vmatrix}$  看成  $A_r$  的函数, 那末  $D_r: \mathfrak{M}(r, K) \rightarrow K$ ,

(i)  $D_r^k \in \mathfrak{L}(K^r, K)$ , (ii) 如果  $r(A) < r$ , 那就  $D_r(A) = 0$ . 因此①

$$D_r = |A_r| \begin{vmatrix} E_r & O \\ O & B_s \end{vmatrix}.$$

同样

$$\begin{vmatrix} E_r & O \\ O & B_s \end{vmatrix} = |B_s| \begin{vmatrix} E_r & O \\ O & E_s \end{vmatrix} = |B_s|, \text{ 所以 } D_r = |A_r| \cdot |B_s|.$$

**系 1**  $D_n(F) = D_n({}^t F) = \sum \operatorname{sgn}(\nu_1, \nu_2, \dots, \nu_n) \alpha_{1\nu_1} \alpha_{2\nu_2} \cdots \alpha_{n\nu_n}.$

**证明** 假如命  $D_n({}^t F) = \mathfrak{D}_n(F)$ , 那末  $\mathfrak{D}_n: \mathfrak{M}(n, K) \rightarrow K$ .

(i) 因为命题 29 的  $\mathfrak{D}_n^k$  是把命题 26 之前定义的  ${}^k D_n \in \mathfrak{L}({}^n K, K)$  “纵看”, 所以  $\mathfrak{D}_n^k \in \mathfrak{L}(K^n, K)$ .

---

① 这时  $D_r(K_r) = \begin{vmatrix} E_r & O \\ O & B_s \end{vmatrix}$ ,  $\mathfrak{D}_r(A_r) = \begin{vmatrix} A_r & O \\ O & B_r \end{vmatrix}$ , 所以  $D_r = |A_r| \begin{vmatrix} E_r & O \\ O & B_s \end{vmatrix}$ .

(ii) 假如  $r(F) < n$ , 因为  $r({}^tF) = r(F) < n$ , 所以

$$\mathfrak{D}_n(F) = D_n({}^tF) = 0.$$

于是

$$D_n({}^tF) = D_n(F) D_n({}^tE_n) = D_n(F) D_n(E_n) = D_n(F).$$

由命题 28 系 2,

$$D_n({}^tF) = \sum \operatorname{sgn}(\nu_1, \nu_2, \dots, \nu_n) \alpha_{1\nu_1} \alpha_{2\nu_2} \cdots \alpha_{n\nu_n}.$$

$$\text{例 4} \quad \begin{pmatrix} \alpha_{11} & \alpha_{12} & \alpha_{13} & \cdots & \alpha_{1n} \\ 0 & \alpha_{22} & \alpha_{23} & \cdots & \alpha_{2n} \\ 0 & 0 & \alpha_{33} & \cdots & \alpha_{3n} \\ \vdots & & & & \vdots \\ 0 & 0 & 0 & \cdots & \alpha_{nn} \end{pmatrix} = \alpha_{11} \alpha_{22} \cdots \alpha_{nn}. \quad (\text{第 2 三角型}).$$

$$\text{例 5} \quad \begin{vmatrix} A_r & O_{r,s} \\ C & B_s \end{vmatrix} = \begin{vmatrix} A_r & C \\ O_{s,r} & B_s \end{vmatrix} = |A_r| \cdot |B_s|.$$

**系 2**  $D_n(F_1 F_2) = D_n(F_1) D_n(F_2).$

**証明** 固定  $F_1$ , 命  $D_n(F_1 F_2) = \mathfrak{D}_n(F_2)$ , 那末  $\mathfrak{D}_n: \mathfrak{M}(n, K) \rightarrow K$ .

$$(i) \quad \text{假定 } F_1 = \begin{pmatrix} {}_1b \\ {}_2b \\ \vdots \\ {}_nb \end{pmatrix}, \quad F_2 = (a_1, a_2, \dots, a_n), \text{ 那末}$$

$$F_1 F_2 = \begin{pmatrix} {}_1ba_1 & {}_1ba_2 & \cdots & {}_1ba_n \\ {}_2ba_1 & {}_2ba_2 & \cdots & {}_2ba_n \\ \vdots & \vdots & & \vdots \\ {}_nba_1 & {}_nba_2 & \cdots & {}_nba_n \end{pmatrix},$$

所以

$$\mathfrak{D}_n^k \in \mathfrak{L}(K_n, K).$$

(ii) 假如  $r(F_2) < n$ , 那末  $r(F_1 F_2) \leq r(F_2) < n$ . 所以

$$\mathfrak{D}_n(F_2) = D_n(F_1 F_2) = 0.$$

于是  $\mathfrak{D}_n$  满足命题 30 中条件, 因此

$$\begin{aligned} D_n(F_1 F_2) &= \mathfrak{D}_n(F_2) = D_n(F_2) \mathfrak{D}_n(E_n) \\ &= D_n(F_2) D_n(F_1 E_n) = D_n(F_1) D_n(F_2). \end{aligned}$$

**系 3** 假如  $F$  正則, 那末  $D_n(F) \neq 0$ .

**証明** 假定  $F$  正則, 那末存在  $F^{-1}$  并且  $FF^{-1} = E_n$ , 所以  $D_n(F) D_n(F^{-1}) = D_n(E_n) = 1$ . 因此  $D_n(F) \neq 0$ .

由命題 27 系 2 及上面的命題 29 系 3, 即得下面定理, 它解答了在本节开始提出的第一个問題。

**定理 14** 矩陣  $F$  是正則的必要充分条件是它的行列式  $|F|$  不等于 0.

除去矩陣  $F = (\alpha_{ik})$  中第  $i$  行及第  $k$  列的元素所得的  $(n-1, n-1)$  型矩陣的行列式, 叫做  $D_n(F)$  的  $(i, k)$  **子行列式**, 記为  $A_{ik}$ . 由命題 27 及命題 29 系 1, 因为矩陣中任意两行互換, 它的行列式只是改变符号, 所以

$$\begin{aligned} D_n(F) &= D_n \begin{pmatrix} {}_1b \\ {}_2b \\ \vdots \\ {}_ib \\ \vdots \\ {}_nb \end{pmatrix} = (-1)^{i-1} D_n \begin{pmatrix} {}_1b \\ {}_2b \\ \vdots \\ {}_{i-1}b \\ {}_{i+1}b \\ \vdots \\ {}_nb \end{pmatrix} \\ &= (-1)^{i-1} \sum_{k=1}^n (-1)^{1+k} \alpha_{ik} A_{ik} = \sum_{k=1}^n \alpha_{ik} (-1)^{i+k} A_{ik}. \end{aligned}$$

$(-1)^{i+k} A_{ik}$  叫做  $\alpha_{ik}$  的**余因子**, 用  $A_{ik}$  表示。由上面的結果即得下命題。它的后半段由命題 29 系 1 自明。

$$\begin{aligned} \text{命題 30 } D_n(F) &= \sum_{k=1}^n \alpha_{ik} A_{ik} \quad (\text{第 } i \text{ 行展开}) \\ &= \sum_{i=1}^n \alpha_{ik} A_{ik} \quad (\text{第 } k \text{ 行展开}). \end{aligned}$$

系  $\sum_{k=1}^n \alpha_{ik} A_{jk} = \delta_{ij} D_n(F)$ ,  $\sum_{i=1}^n \alpha_{ik} A_{il} = \delta_{kl} D_n(F)$ .

证明 当  $i=j$  时, 由本命题即得。

当  $i \neq j$  时,  $\sum \alpha_{ik} A_{jk}$  是  $F$  的第  $j$  行换成  $(\alpha_{i1}, \alpha_{i2}, \dots, \alpha_{in})$  所成矩阵的行列式依第  $j$  行的展开, 但这行列式第  $i$  行与第  $j$  行相等, 所以等于 0.

**定理 15** 矩阵  $F$  是正则时, 假如它的第  $(i, k)$  元素的余因子是  $A_{ik}$ , 那末

$$F^{-1} = \frac{1}{D_n(F)} {}^t(A_{ik}).$$

证明 假定  $F = (\alpha_{ik})$ , 那末

$$\begin{aligned} (\alpha_{ik}) \cdot \frac{1}{D_n(F)} {}^t(A_{ik}) &= \frac{1}{D_n(F)} \left( \sum_{j=1}^n \alpha_{ij} A_{kj} \right) \\ &= \frac{1}{D_n(F)} (\delta_{ik} D_n(F)) = (\delta_{ik}) = E_n. \end{aligned}$$

因此(参照 § 7, 例 12),

$$F^{-1} = \frac{1}{D_n(F)} {}^t(A_{ik}). \quad (\text{证毕})$$

定理 15 解答了在本节开始提出的第二个问题。

**例 6**  $D_n(F) = D_n(a_1 a_2 \cdots a_n) = D_n(a_1 a_2 + \lambda_1 a_1 a_3 + \lambda_2 a_1 \cdots a_n + \lambda_{n-1} a_1)$ ,

$$D_n(F) = D_n \begin{pmatrix} 1b \\ 2b \\ 3b \\ \vdots \\ nb \end{pmatrix} = D_n \begin{pmatrix} 1b \\ 2b + \mu_1 1b \\ 3b + \mu_2 1b \\ \dots\dots\dots \\ nb + \mu_{n-1} 1b \end{pmatrix}.$$

在实际计算行列式时, 可适当挑选上面的  $\lambda_k$  或  $a_i$ , 使得 1 列或 1 行中元素只剩下一个而其他都是 0, 然后依这列或这行展开。

$$\begin{vmatrix} 1 & 1 & -3 & 4 \\ 0 & 2 & 1 & -2 \\ 3 & 2 & -4 & 1 \\ -3 & 1 & 0 & -1 \end{vmatrix} = \begin{vmatrix} 1 & 1 & -3 & 4 \\ 0 & 2 & 1 & -2 \\ 0 & -1 & 5 & -11 \\ 0 & 4 & -9 & 11 \end{vmatrix} = \begin{vmatrix} 2 & 1 & -2 \\ -1 & 5 & -11 \\ 4 & -9 & 11 \end{vmatrix}$$

$$= \begin{vmatrix} 0 & 1 & 0 \\ -11 & 5 & -1 \\ 22 & -9 & -7 \end{vmatrix} = - \begin{vmatrix} -11 & -1 \\ 22 & -7 \end{vmatrix} = 11 \begin{vmatrix} -1 & 1 \\ 2 & 7 \end{vmatrix} \\ = -11 \times (-9) = -99.$$

**例7** 当  $F$  是正则矩阵时, 1 次方程  $Fx=y$  的解是由  $x=F^{-1}y$  给出(命题 23)。引用定理 15,

$$x = \frac{t(A_{ik})y}{D_n(F)}.$$

因此, 假如

$$x = \begin{pmatrix} \xi_1 \\ \vdots \\ \xi_n \end{pmatrix}, \quad y = \begin{pmatrix} \eta_1 \\ \vdots \\ \eta_n \end{pmatrix}, \quad \text{那末 } \xi_l = \frac{\sum_{i=1}^n A_{li} \eta_i}{D_n(F)}. \quad (1)$$

这里分子是  $F$  的第  $l$  列换成  $\begin{pmatrix} \eta_1 \\ \vdots \\ \eta_n \end{pmatrix}$  所成矩阵的行列式。

(1) 叫做 **Cramer 公式**。

在以下的例 8 和例 9 中, 假定  $K=\mathbf{R}$ 。

$$\text{例 8} \quad \begin{cases} \xi_1 + \xi_2 - 3\xi_3 + 4\xi_4 = 5, \\ 2\xi_2 + \xi_3 - 2\xi_4 = 0, \\ 3\xi_1 + 2\xi_2 - 4\xi_3 + \xi_4 = 16, \\ -3\xi_1 + \xi_2 \quad \quad - \xi_4 = -8. \end{cases}$$

即

$$F = \begin{pmatrix} 1 & 1 & -3 & 4 \\ 0 & 2 & 1 & -2 \\ 3 & 2 & -4 & 1 \\ -3 & 1 & 0 & -1 \end{pmatrix}, \quad y = \begin{pmatrix} 5 \\ 0 \\ 16 \\ -8 \end{pmatrix}.$$

[解]  $D_n(F) = -99 \neq 0$  (例 6), 因此这联立方程是正则。由 Cramer 公式得

$$\xi_1 = \frac{1}{-99} \begin{vmatrix} 5 & 1 & -3 & 4 \\ 0 & 2 & 1 & -2 \\ 16 & 2 & -4 & 1 \\ -8 & 1 & 0 & -1 \end{vmatrix} = 3.$$

同样

$$\xi_2 = 0, \quad \xi_3 = -2, \quad \xi_4 = -1.$$

例 9

$$\begin{cases} \xi_1 + 2\xi_2 - 3\xi_3 - 4\xi_4 = \alpha, \end{cases} \quad (1)$$

$$\begin{cases} -\xi_1 + 3\xi_2 + \xi_3 + 2\xi_4 = \beta, \end{cases} \quad (2)$$

$$\begin{cases} \xi_1 + 7\xi_2 - 5\xi_3 - 6\xi_4 = \gamma, \end{cases} \quad (3)$$

即

$$F = \begin{pmatrix} 1 & 2 & -3 & -4 \\ -1 & 3 & 1 & 2 \\ 1 & 7 & -5 & -6 \end{pmatrix}, \quad y = \begin{pmatrix} \alpha \\ \beta \\ \gamma \end{pmatrix}.$$

$$[\text{解}] \quad r(F) = r \begin{pmatrix} 1 & 2 & -3 & -4 \\ -1 & 3 & 1 & 2 \\ 1 & 7 & -5 & -6 \end{pmatrix} = r \begin{pmatrix} 1 & 2 & -3 & -4 \\ 0 & 5 & -2 & -2 \\ 0 & 5 & -2 & -2 \end{pmatrix}. \quad (4)$$

(把  $F$  的第一行加于第二行, 又自第三行减去第一行即得右边的矩阵。)  
在此

$$\begin{vmatrix} 1 & 2 \\ 0 & 5 \end{vmatrix} = 5 \neq 0. \quad (5)$$

由(4)的变形, 自  $F$  所作的三次行列式显然都成为 0, 所以

$$r(F) = 2, \quad (6)$$

因此, 所给方程组有解的条件是

$$r(F_1) = r \begin{pmatrix} 1 & 2 & -3 & -4 & \alpha \\ -1 & 3 & 1 & 2 & \beta \\ 1 & 7 & -5 & -6 & \gamma \end{pmatrix} = 2. \quad (7)$$

但象(4)这样的变形(因为没有行、列的互换),  $F$  的主部位置不变(请读者考虑)。因此, 由(5), (6)得知  $F_1$  的第一列、第二列是无关, 第三列、第四列应该是它们的线性组合。所以条件(7)等价于

$$\begin{vmatrix} 1 & 2 & \alpha \\ -1 & 3 & \beta \\ 1 & 7 & \gamma \end{vmatrix} = 0 \quad \text{即} \quad 2\alpha + \beta = \gamma. \quad (7')$$

于是在(7')的条件下, 用定理 13 解方程组(1), (2), (3)。但由(5), (6), 这方程组与(1), (2)两个等价。

$$F_0 = \begin{pmatrix} 1 & 2 \\ -1 & 3 \end{pmatrix}, \quad F_* = \begin{pmatrix} -3 & -4 \\ 1 & 2 \end{pmatrix} \quad (\text{定理 13 的记法}),$$

$$|F_0| = 5, \quad \text{所以} \quad F_0^{-1} = \frac{1}{5} \begin{pmatrix} 3 & -2 \\ 1 & 1 \end{pmatrix}.$$

$$\text{因此,} \quad F_0^{-1}y = \frac{1}{5} \begin{pmatrix} 3 & -2 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \frac{1}{5} \begin{pmatrix} 3\alpha - 2\beta \\ \alpha + \beta \end{pmatrix}.$$

所以特殊解

$$x_0 = \begin{pmatrix} \frac{1}{5}(3\alpha - 2\beta) \\ \frac{1}{5}(\alpha + \beta) \\ 0 \\ 0 \end{pmatrix}.$$

又 
$$F_0^{-1}F_* = \frac{1}{5} \begin{pmatrix} 3 & -2 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} -3 & -4 \\ 1 & 2 \end{pmatrix} = \frac{1}{5} \begin{pmatrix} -11 & -16 \\ -2 & -2 \end{pmatrix},$$

所以

$$\begin{pmatrix} F_0^{-1}F_* \\ -E_2 \end{pmatrix} = \begin{pmatrix} -\frac{11}{5} & -\frac{16}{5} \\ -\frac{2}{5} & -\frac{2}{5} \\ -1 & 0 \\ 0 & -1 \end{pmatrix}.$$

于是一般解

$$x = \begin{pmatrix} \xi_1 \\ \xi_2 \\ \xi_3 \\ \xi_4 \end{pmatrix} = \begin{pmatrix} \frac{1}{5}(3\alpha - 2\beta) \\ \frac{1}{5}(\alpha + \beta) \\ 0 \\ 0 \end{pmatrix} - \lambda \begin{pmatrix} \frac{11}{5} \\ \frac{2}{5} \\ 1 \\ 0 \end{pmatrix} - \mu \begin{pmatrix} \frac{16}{5} \\ \frac{2}{5} \\ 0 \\ 1 \end{pmatrix}.$$

这里  $\lambda, \mu$  是在  $K = \mathbf{R}$  上变动的参数元。

### § 13 綫性变换及其不变子空間

如前所述, 体  $K$  上向量空間  $V$  到它自身的綫性映射叫做  $V$  的綫性变换, 它們全体的集合  $\mathfrak{L}(V, V) = \mathfrak{L}(V)$ , 是  $K$  上代数 (§7, 命題 8)。在  $V$  取坐标系  $\varphi$ , 于是  $\mathfrak{L}(V)$  中元  $f$  可以用  $\mathfrak{M}(n, K)$  中元  $F$  表示 (§8)。因此, 要使  $f$  的性质明显易得, 就需要适当取  $\varphi$  使  $F$  的形状尽可能简单。假如坐标系自  $\varphi$  变为  $\psi$ , 坐标变换的 (正則) 矩陣是  $P$ , 那末表示  $f$  的矩陣自  $F$  变为  $PF P^{-1}$ 。把  $F$  变换为  $PF P^{-1}$  这个事实叫做用  $P$  变换  $F$ 。当  $F_1, F_2 \in \mathfrak{M}(n, K)$  时, 假如存在适合  $F_2 = PF_1 P^{-1}$  这样的  $n$  級正則矩陣  $P$ , 那末  $F_1$ ,



$F_2$  叫做相似, 写成  $F_1 \sim F_2$ . 相似关系显然是等价关系. 适当取  $\varphi$  使表示  $f$  的矩阵简单化这个问题, 假如作为矩阵的问题来考虑, 那就与“变换所给出的矩阵  $F$  使它的形状尽可能简单的问题”或“求与  $F$  相似且形状尽可能简单的矩阵的问题”相同. 这问题的一般解答将在 §15 给出. 这里为了简便叫它做“问题 A”. 在讨论这问题 A 时, 下述的不变子空间的概念是需要的.

以下首先固定  $V$  及  $\mathfrak{L}(V)$  中元  $f$  来考虑.  $V$  的子空间  $W$  叫做对于  $f$  不变或  $f$  的不变子空间, 其意义是  $f(W) \subset W$ . 因为  $f$  固定, 所以  $f$  的不变子空间有时也单称为不变子空间.  $f$  的不变子空间全体的集合用  $\mathfrak{W}_f$  或简略地用  $\mathfrak{W}$  表示 (例:  $\mathfrak{W} \in \{0, V\}$ ).

**命题 31** 假定  $W_1 \in \mathfrak{W}$ , 那末  $f$  到  $W_1$  的缩小  $f_1 = f|_{W_1} \in \mathfrak{L}(W_1)$ .

**证明** 对于  $x, y \in W_1$ ,  $f_1(x) = f(x)$ ,  $f_1(y) = f(y)$ , 因此  $f_1(x+y) = f(x+y) = f(x) + f(y) = f_1(x) + f_1(y)$ . 同样  $f_1(\lambda x) = \lambda f_1(x)$ .

**命题 32** 当  $W_1, V/W_1 = V^{(1)} \in \mathfrak{W}$  时, 假如对于  $(x)_{W_1} \in V^{(1)}$ , 使  $(f(x))_{W_1} \in V^{(1)}$  与之对应的映射是  $f^{(1)}$ , 那末  $f^{(1)} \in \mathfrak{L}(V^{(1)})$ .

**证明** 设  $(x)_{W_1} = (y)_{W_1}$ , 即  $x \equiv y \pmod{W_1}$ , 因为  $x - y \in W_1$ ,  $W_1 \in \mathfrak{W}$ , 所以  $f(x - y) \in f(W_1) \subset W_1$ . 于是  $f(x) \equiv f(y) \pmod{W_1}$ ,  $(f(x))_{W_1} = (f(y))_{W_1}$ . 因此  $f^{(1)}$  的确可以定义为把  $V^{(1)}$  映于  $V^{(1)}$  的映射 (以下省略  $(x)_{W_1}$  中的  $W_1$  单记为  $(x)$ ). 再因为  $(x) + (y) = (x + y)$ ,  $\lambda(x) = (\lambda x)$ , 所以  $f^{(1)}((x) + (y)) = f^{(1)}((x + y)) = (f(x + y)) = (f(x) + f(y)) = (f(x)) + (f(y)) = f^{(1)}((x)) + f^{(1)}((y))$ . 同样,  $f^{(1)}(\lambda(x)) = \lambda f^{(1)}((x))$ . 所以  $f^{(1)} \in \mathfrak{L}(V^{(1)})$ .

**命题 33** 假定  $V$  是有限维, 如果  $\dim V = n$ ,  $W_1 \in \mathfrak{W}$ ,  $0 < \dim W_1 = r_1 < n$ ,  $n = r_1 + r^{(1)}$  (因此  $0 < r^{(1)} < n$ ). 而  $\{a_1, a_2, \dots, a_{r_1}\}$  是  $W_1$  的一个基底, 由 §5 定理 5 系 4,  $V$  的基底可以取  $\{a_1, a_2,$

$\cdots, a_{r_1}, a_{r_1+1}, \cdots, a_n\}$  形状, 那末对于坐标系  $\varphi = \varphi(a_1, a_2, \cdots, a_n)$ ,  $f$  能够用下面形状的矩阵来表示:

$$\begin{pmatrix} F_1 & G \\ \xleftrightarrow[r_1]{O_{r(1), r_1}} & \xleftrightarrow[r(2)]{F^{(1)}} \end{pmatrix} \begin{matrix} \uparrow r_1 \\ \uparrow r(2) \end{matrix} \quad (13.1)$$

这里  $F_1$  是对于  $W_1$  的基底  $\{a_1, a_2, \cdots, a_{r_1}\}$  表示  $f_1 = f|_{W_1}$  的矩阵,  $F^{(1)}$  是对于  $V^{(1)}$  的基底  $\{(a_{r_1+1}), \cdots, (a_n)\}$  表示  $f^{(1)}$  的矩阵。

**证明** 因为  $f(a_1), f(a_2), \cdots, f(a_{r_1}) \in f(W_1) \subset W_1$ , 所以在表示  $f$  的矩阵的最初  $r_1$  列中后面的  $r^{(1)}$  个元素都是 0. 但  $f_1(a_1) = f(a_1), \cdots, f_1(a_{r_1}) = f(a_{r_1})$ , 所以  $F_1$  是对于  $\{a_1, \cdots, a_{r_1}\}$  表示  $f_1$  的矩阵。

再对于  $F$  中剩下的  $r^{(1)}$  列, 譬如设  $f(a_{r_1+1}) = \sum_{i=1}^n \lambda_i a_i$ , 因为  $f^{(1)}((a_{r_1+1})) = (f(a_{r_1+1})) = \left(\sum_{i=1}^n \lambda_i a_i\right) = \left(\sum_{i=r_1+1}^n \lambda_i a_i\right) = \sum_{i=r_1+1}^n \lambda_i (a_i)$ , 所以  $F^{(1)}$  是对于  $\{(a_{r_1+1}), \cdots, (a_n)\}$  表示  $f^{(1)}$  的矩阵。

**系** 假如  $V^{(1)}$  的  $r_2$  维子空间  $W_2$  对于  $f^{(1)}$  不变,  $r^{(1)} = r_2 + r^{(2)}$  (假如必要, 和以前一样变动记法), 如果  $W_2$  的基底是  $\{(a_{r_1+1}), \cdots, (a_{r_1+r_2})\}$ ,  $V^{(1)}$  含它的基底是  $\{(a_{r_1+1}), \cdots, (a_n)\}$ , 那末对于  $V$  的基底  $\{a_1, a_2, \cdots, a_n\}$ ,  $f$  能够用

$$\begin{pmatrix} F_1 & * & * \\ 0 & F_2 & * \\ 0 & 0 & F^{(2)} \end{pmatrix} \begin{matrix} \uparrow r_1 \\ \uparrow r_2 \\ \uparrow r^{(2)} \end{matrix} \quad (13.2)$$

$\xleftrightarrow[r_1]{} \quad \xleftrightarrow[r_2]{} \quad \xleftrightarrow[r^{(2)}]{} \quad$

形状的矩阵表示。

**命题 34** 假定  $V = W_1 \oplus W_2$ ,  $W_i \in \mathfrak{B}$  ( $i=1, 2$ ),  $\dim V = n$ ,  $\dim W_i = r_i$ , 因此  $n = r_1 + r_2$ ,  $0 < r_i < n$  ( $i=1, 2$ ). 如果  $W_1 = [a_1, \cdots, a_{r_1}]$ ,  $W_2 = [a_{r_1+1}, \cdots, a_n]$ , 于是  $\{a_1, \cdots, a_n\}$  成为  $V$  的一个基

底, 假如  $\varphi = \varphi(a_1, \dots, a_n)$ , 那末对于  $\varphi, f$  能够用下面形状的矩陣表示:

$$\begin{pmatrix} F_1 & O_{r_2, r_1} \\ O_{r_1, r_2} & F_2 \end{pmatrix}, \quad (13.3)$$

这里  $F_i$  是对于基底  $\{a_1, \dots, a_{r_i}\}$  或  $\{a_{r_1+1}, \dots, a_n\}$  表示  $f_i = f|W_i$  的矩陣。

**証明** 与命题 33 証明的前半段同样考察即可明白。

**系** 假定  $V = W_1 \oplus W_2 \oplus \dots \oplus W_k$ ,  $W_i \in \mathfrak{B}$  ( $i = 1, 2, \dots, k$ ),  $\dim V = n$ ,  $\dim W_i = r_i$ , 因此  $n = r_1 + r_2 + \dots + r_k$ ,  $0 < r_i < n$  ( $i = 1, 2, \dots, k$ ). 如果  $W_1 = [a_1, \dots, a_{r_1}]$ ,  $W_2 = [a_{r_1+1}, \dots, a_{r_1+r_2}]$ ,  $\dots$ ,  $W_k = [a_{r_1+\dots+r_{k-1}}, \dots, a_n]$ , 于是  $\{a_1, \dots, a_n\}$  成为  $V$  的一个基底, 假如  $\varphi = \varphi(a_1, \dots, a_n)$ , 那末对于  $\varphi, f$  能够用下面形状的矩陣表示:

$$\begin{pmatrix} F_1 & O & \dots & O \\ O & F_2 & \dots & O \\ \vdots & \vdots & \ddots & \vdots \\ O & O & \dots & F_k \end{pmatrix} \begin{matrix} \downarrow r_1 \\ \downarrow r_2 \\ \vdots \\ \downarrow r_k \end{matrix} \quad (13.4)$$

$$\begin{matrix} \xleftarrow{r_1} & \xleftarrow{r_2} & \dots & \xleftarrow{r_k} \end{matrix}$$

假定对于  $W_i$  的基底  $\{a_{r_1+\dots+r_{i-1}+1}, \dots, a_{r_1+\dots+r_i}\}$  的坐标系是  $\varphi_i$ , 那末对于  $\varphi_i$ , 表示  $f_i = f|W_i$  的矩陣是  $F_i$ .

(13.4) 的矩陣今后用  $F_1 \oplus F_2 \oplus \dots \oplus F_k$  表示。假如  $V$  能够分解为不变子空間  $W_i$  的直和, 那末由上系, 問題 A 就归結为各个比原来維数低的  $W_i$  的問題。

## § 14 特征值, 特征多項式, Cayley-Hamilton 定理

假定  $V$  是体  $K$  上向量空間,  $f \in \mathfrak{L}(V)$ ,  $\alpha \in K$ , 对于  $V$  中非 0 元  $x$ , 如果

$$f(x) = \alpha x, \quad (14.1)$$

那末  $\alpha$  叫做  $f$  的特征值。  $x$  叫做  $f$  属于特征值  $\alpha$  的特征向量。

**例 1** 假定  $V = \mathfrak{L}(C)$ ,  $\Delta = D^n + p_1 D^{n-1} + \cdots + p_{n-1} D + p_n$ , 那末微分方程  $\Delta y = \alpha y$  中异于  $y=0$  的解  $\alpha \in C$  是  $\Delta$  的特征值, 这时解  $y$  是  $\Delta$  属于  $\alpha$  的特征向量。

**命题 35** 假定  $\alpha$  是  $f \in \mathfrak{L}(V)$  的特征值,  $\alpha$  的特征向量全体及 0 的集合是  $W(\alpha)$ , 当  $\alpha$  不是  $f$  的特征值时命  $W(\alpha) := \{0\}$ , 那末  $W(\alpha) \in \mathfrak{B}_f$ . ( $W(\alpha)$  叫做  $\alpha$  的特征空间)

**证明** 因为  $W(\alpha) = \text{Ker}(f - \alpha)$ , 所以  $W(\alpha)$  是  $V$  的子空间。又假如  $x \in W(\alpha)$ , 那末  $f(x) = \alpha x$ , 因此  $f^2(x) = f(\alpha x) = \alpha f(x)$ . 于是  $f(x) \in W(\alpha)$ , 即  $f(W(\alpha)) \subset W(\alpha)$ . 所以  $W(\alpha) \in \mathfrak{B}_f$ .

本命题能够象下面那样一般化。

因为  $\mathfrak{L}(V)$  是  $K$  上代数, 假如  $f \in \mathfrak{L}(V)$ , 那末  $f \cdot f = f^2$ ,  $f \cdot f^2 = f^3$ ,  $\cdots$ ,  $f \cdot f^{v-1} = f^v$  也是  $\mathfrak{L}(V)$  中元, 又假如  $\alpha_0, \alpha_1, \cdots, \alpha_v \in K$ , 那末  $\alpha_0 + \alpha_1 f + \cdots + \alpha_v f^v \in \mathfrak{L}(V)$ . 它可以看成把  $f$  “代入”  $K$  上 (即以  $K$  中元做系数) 变数  $X$  之多项式  $\Phi(X) := \alpha_0 + \alpha_1 X + \cdots + \alpha_v X^v$  中的结果, 写成  $\Phi(f) = \alpha_0 + \alpha_1 f + \cdots + \alpha_v f^v$ . 显然

$$f \cdot \Phi(f) = \Phi(f) \cdot f. \quad (14.2)$$

**命题 36**  $\text{Ker } \Phi(f) \in \mathfrak{B}_f$  (当  $\Phi(f) = f - \alpha$  时, 即为上命题)。

**证明** 因为  $\Phi(f) \in \mathfrak{L}(V)$ , 所以  $\text{Ker } \Phi(f)$  是  $V$  的子空间。今设  $W = \text{Ker } \Phi(f)$ . 如果  $x \in W$ , 那末  $\Phi(f)(x) = 0$ . 命  $f(x) = y$ , 引用 (14.2),  $\Phi(f)(y) = \Phi(f)(f(x)) = f(\Phi(f)(x)) = 0$ . 所以  $y \in W$ ,  $f(W) \subset W$ . (证毕)

以下假定  $V$  是有限维的,  $\dim V = n$ , 来考虑前节提出的问题 A. 因为  $W(\alpha)$  是  $\mathfrak{B}$  中元, 由前节命题 33, 34, 当然能够使问题简化, 但是如果  $\alpha$  不是特征值, 就会有  $\dim W(\alpha) = 0$  的结果。因此求特征值成为重要问题。  $f$  的特征值全体的集合用  $\mathfrak{E}_f$  或  $\mathfrak{E}$  表示。

**例2**  $\dim W(\alpha) = n$  时,  $V = W(\alpha)$ , 不論  $V$  的坐标系如何选取, 表示  $f$  的矩陣是  $\alpha E$ .

**命题37** 假定对于某坐标系表示  $f$  的矩陣是  $F$ , 那末

$$\alpha \in \mathbb{C} \Rightarrow |\alpha E - F| = 0.$$

**証明** 假定  $x_0$  是属于  $\alpha$  的一个特征向量, 那末  $f(x_0) = \alpha x_0$ . 所以  $(\alpha E - F)x_0 = \alpha x_0 - f(x_0) = 0$ . 于是  $n$  元联立1次方程  $(\alpha E - F)x = 0$  的解构成維数大于1的子空間, 所以  $r(\alpha E - F) \leq n-1$ . 因此  $|\alpha E - F| = 0$ . (証毕)

由上面証明, 即可推得下面的系。

**系**  $\alpha \in \mathbb{C}$  时,  $\dim W(\alpha) = d(\alpha E - F) = n - r(\alpha E - F)$ , 其中  $d$  表示退化次数,  $r$  表示秩。

假定  $F$  是  $n$  級方陣, 那末

$$\Phi_F(X) = |XE - F|$$

是  $K$  上变数  $X$  的  $n$  次多項式。它叫做矩陣  $F$  的特征多項式。

**例3** 在行列式  $|F|$  的子行列式中, 其主对角綫上元素都是  $|F|$  的主对角綫上元素者, 叫做  $|F|$  的主子式, 即

$$|F| = \begin{vmatrix} \alpha_{11} & \alpha_{12} & \cdots & \alpha_{1n} \\ \alpha_{21} & \alpha_{22} & \cdots & \alpha_{2n} \\ \vdots & \vdots & & \vdots \\ \alpha_{n1} & \alpha_{n2} & \cdots & \alpha_{nn} \end{vmatrix} \text{ 时, } \begin{vmatrix} \alpha_{p_1 p_1} & \alpha_{p_1 p_2} & \cdots & \alpha_{p_1 p_k} \\ \alpha_{p_2 p_1} & \alpha_{p_2 p_2} & \cdots & \alpha_{p_2 p_k} \\ \vdots & \vdots & & \vdots \\ \alpha_{p_k p_1} & \alpha_{p_k p_2} & \cdots & \alpha_{p_k p_k} \end{vmatrix}$$

形状的行列式是  $|F|$  的主子式。  $|F|$  的  $r$  次主子式全体的和如果写为  $S_r(F)$ , 那末<sup>①</sup>

$$\Phi_F(X) = X^n - S_1(F) \cdot X^{n-1} + S_2(F) \cdot X^{n-2} + \cdots + (-1)^n S_n(F),$$

<sup>①</sup> 由行列式的基本性质,  $\Phi_F(X)$  可以分解为  $2^n$  个  $n$  級行列式的和, 即

$$\begin{aligned} \Phi_F(X) = |XE - F| &= \begin{vmatrix} X - \alpha_{11} & 0 & \cdots & 0 - \alpha_{1n} \\ 0 & X - \alpha_{22} & \cdots & 0 - \alpha_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ 0 - \alpha_{n1} & 0 - \alpha_{n2} & \cdots & X - \alpha_{nn} \end{vmatrix} \\ &= |XE| + \sum_{k=1}^n \sum_{1 \leq i_1 < \cdots < i_k \leq n} D(i_1 \cdots i_k), \quad (\text{續下頁脚注}) \end{aligned}$$

这里  $S_n(F) = |F|$ ,  $S_1(F) = a_{11} + a_{22} + \cdots + a_{nn}$ . 把  $S_1(F)$  写成  $S(F)$ , 叫做  $F$  的迹 (spur 或 trace)。

**例 4** 假定  $K = \mathbb{C}$ , 求  $F = \begin{pmatrix} 1 & 2 & 2 \\ 1 & -1 & 1 \\ 4 & -12 & 1 \end{pmatrix}$  的特征多项式, 特征值及属于各特征值的特征空间。

**[解]**  $S(F) = 1 + (-1) + 1 = 1$ ,

$$S_2(F) = \begin{vmatrix} 1 & 2 \\ 1 & -1 \end{vmatrix} + \begin{vmatrix} -1 & 1 \\ -12 & 1 \end{vmatrix} + \begin{vmatrix} 1 & 2 \\ 4 & 1 \end{vmatrix} \\ = -1 - 2 - 1 + 12 + 1 - 8 = 1,$$

$$|F| = \begin{vmatrix} 1 & 2 & 2 \\ 1 & -1 & 1 \\ 4 & -12 & 1 \end{vmatrix} = \begin{vmatrix} 1 & 0 & 0 \\ 1 & -3 & -1 \\ 4 & -20 & -7 \end{vmatrix} = 21 - 20 = 1,$$

所以特征多项式

$$\phi_F(X) = X^3 - X^2 + X - 1.$$

$F$  的特征值可以作为  $\phi_F(X) = 0$  的根来求。由  $X^3 - X^2 + X - 1 = (X - 1) \cdot (X^2 + 1) = (X - 1)(X - i)(X + i)$ , 得  $\mathbb{C} = \{1, i, -i\}$ 。

求  $W(1)$ , 解  $Fx = x$  或  $(E - F)x = 0$  即可。

$$\text{假定 } x = \begin{pmatrix} \xi_1 \\ \xi_2 \\ \xi_3 \end{pmatrix}, \text{ 那末 } \begin{cases} -2\xi_2 - 2\xi_3 = 0, \\ -\xi_1 + 2\xi_3 - \xi_3 = 0, \\ -4\xi_1 + 12\xi_2 = 0, \end{cases}$$

解之, 得

$$W(1) = \left\{ \lambda \begin{pmatrix} 3 \\ 1 \\ -1 \end{pmatrix}; \lambda \in \mathbb{C} \right\}.$$

同样

$$\text{解 } Fx = ix, \text{ 得 } W(i) = \left\{ \lambda \begin{pmatrix} 4 + 2i \\ 1 + i \\ -4 \end{pmatrix}; \lambda \in \mathbb{C} \right\},$$

(续上页) 这里  $D(i_1, \dots, i_k)$  表示  $n$  级行列式, 它的第  $i_1, \dots, i_k$  列分别是  $-F$  的第  $i_1, \dots, i_k$  列而其余的  $n - k$  列 (如果存在, 即当  $k < n$  时) 分别是矩阵  $\lambda E$  相应的列, 命  $\Delta(i_1, \dots, i_k)$  为  $F$  中取第  $i_1, \dots, i_k$  列和行所成的  $k$  级主子 (行列) 式。于是

$$\phi_F(X) = X^n + \sum_{k=1}^n \sum_{1 \leq i_1 < \dots < i_k \leq n} (-1)^k X^{n-k} \Delta(i_1, \dots, i_k) = X^n \sum_{k=0}^n (-1)^k S_k X^{-k},$$

式中  $S_k$  是  $F$  中所有  $k$  级主子式的和。——译者注

$$\text{解 } Fx = -ix, \text{ 得 } W(-i) = \left\{ \lambda \begin{pmatrix} 4-2i \\ 1-i \\ -4 \end{pmatrix}; \lambda \in \mathbb{C} \right\}.$$

**命題 38** 假定  $P$  是  $n$  級正則矩陣, 那末

$$\Phi_{PF P^{-1}}(X) = \Phi_F(X).$$

$$\begin{aligned} \text{証明 } \Phi_{PF P^{-1}}(X) &= |XE - PF P^{-1}| = |P \cdot XE \cdot P^{-1} - PF P^{-1}| \\ &= |P(XE - F)P^{-1}| = |P| |XE - F| |P^{-1}| \\ &= |XE - F| \cdot |P| \cdot |P^{-1}| = \Phi_F(X) \cdot |PP^{-1}| \\ &= \Phi_F(X). \end{aligned}$$

**系** 用例 3 的記法,  $S_i(PF P^{-1}) = S_i(F)$ , 特別  $S(PF P^{-1}) = S(F)$ .

**命題 39**  $\Phi_{F_1 \oplus F_2 \oplus \dots \oplus F_k} = \Phi_{F_1} \cdot \Phi_{F_2} \cdots \Phi_{F_k},$

$$S(F_1 \oplus F_2 \oplus \dots \oplus F_k) = S(F_1) + \dots + S(F_k).$$

**証明** 假設  $F = F_1 \oplus F_2 \oplus \dots \oplus F_k$ , 那末

$$XE - F = (XE_{r_1} - F_1) \oplus (XE_{r_2} - F_2) \oplus \dots \oplus (XE_{r_k} - F_k)$$

( $r_i$  是  $F_i$  的級数)。于是

$\Phi_F(X) = |XE - F| = \Phi_{F_1}(X) \cdot \Phi_{F_2}(X) \cdots \Phi_{F_k}(X)$  (§ 12 例 3), 比較这式两边含  $X^{n-1}$  ( $n$  是  $F$  的級数) 項的系数, 即得

$$S(F) = S(F_1) + \dots + S(F_k). \quad (\text{証毕})$$

由命題 38 及它的系, 得知  $\Phi_F$  和  $S(F)$  只由  $f$  确定而与坐标系  $\varphi$  无关。事实上, 如果改变坐标系, 那末  $F$  变为  $PF P^{-1}$ , 但  $\Phi_F$  与  $S(F)$  对于这变换不变, 此已由本命題及系揭示。因此把  $\Phi_F, S(F)$  写成  $\Phi_f, S(f)$ 。

$n$  次代数方程  $\Phi_f(X) = 0$  叫做  $f$  或  $F$  的**特征方程** (或由于在天文学上历史的理由而叫做**永年方程** (secular equation))。求  $f$  的特征值解它的特征方程即可。但是这方程的根不一定都在基础体  $K$  中 (譬如在例 4, 因为假定  $K = \mathbb{C}$ , 所以  $\Phi_f(X) = 0$  的根都

在  $K$  中, 但是如果假定  $K = \mathbf{R}$ , 那末  $\Phi_f(X) = 0$  的根  $\pm i$  不含于  $K$ ). 然而由代数学上已知定理 (例如, 正田, 浅野: 代数学 I, 岩波书店, 1952, p. 53), 作含  $K$  的某个体  $K'$ , 在  $K'$  中就能够含  $\Phi_f(X)$  的所有根 [对给定的体  $K$  作适当“扩张体” (当然是含  $K$  的体)  $\bar{K}$  能够使得  $K$  上“任意”代数方程在  $\bar{K}$  中具有根 (正田, 浅野: 代数学 I, p. 54)。例如假定  $K = \mathbf{R}$ , 那末作  $\bar{K} = \mathbf{C}$  即可。根据所谓“代数学的基本定理”以“复数作系数的代数方程的根都在复数体中”]。这时如果  $F \in \mathfrak{M}(n, K)$ , 当然  $F \in \mathfrak{M}(n, K')$ , 因此自始即以  $K'$  为基础体, 那末“特征方程的根都在基础体中”。为了今后简单起见, 假定基础体适当取“大”使这事实能成立。于是显然有下面的命题。

**命题 40**  $\alpha \in \mathfrak{E}_f \Leftrightarrow \Phi_f(\alpha) = 0$ .

假定  $\mathfrak{E}_f = \{\alpha_1, \alpha_2, \dots, \alpha_k\}$ , (当  $i \neq j$  时,  $\alpha_i \neq \alpha_j$ ),

因为  $\Phi_f(X)$  是最高次系数为 1 的  $n$  次多项式,

$$\Phi_f(X) := (X - \alpha_1)^{r_1} (X - \alpha_2)^{r_2} \cdots (X - \alpha_k)^{r_k}, \quad (14.3)$$

$$n = r_1 + r_2 + \cdots + r_k, \quad n \geq r_1 \geq 1, \quad n \geq k \geq 1. \quad (14.4)$$

由命题 36,  $\text{Ker}(f - \alpha_i)^{r_i} \in \mathfrak{B}_f$ . 因为  $\text{Ker}(f - \alpha_i) = W(\alpha_i)$ ,  $\alpha_i \in \mathfrak{E}_f$ , 所以  $\dim \text{Ker}(f - \alpha_i) > 0$ . 但是 “ $\mu \leq \mu' \Rightarrow \dim \text{Ker}(f - \alpha_i)^\mu \leq \dim \text{Ker}(f - \alpha_i)^{\mu'}$ ”, 故  $\dim \text{Ker}(f - \alpha_i)^{r_i} > 0$ . 今命  $\text{Ker}(f - \alpha_i)^\mu = W_{i,\mu}$ ,  $f|W_{i,r_i} = f_i$ , 显然  $W(\alpha_i) = W_{i,1} \subset W_{i,2} \subset \cdots \subset W_{i,r_i} \subset \cdots$ .

**命题 41**  $\dim W_{i,r_i} \geq r_i$ , 适当取  $W_{i,r_i}$  的基底, 能够使表示  $f_i$  的矩阵含下面形状的  $r_i$  级第 2 三角型矩阵:

$$\begin{pmatrix} \alpha_1 & & & \\ & \alpha_i & & * \\ & & \ddots & \\ 0 & & & \alpha_i \end{pmatrix}.$$

**注意** 实际上, 在此假如  $\dim W_{i,r_i} = r_i$ , 自  $W_{i,r_i}$  适当取基底, 那末表示



$f_i$  的矩陣自身就成为上面的形状,这在稍后即知(定理 16 后面的例 5)。

**証明** 因为对于任何  $i$  都一样,所以作为  $i=1$  来証明。 $r_1=1$  时是明显的。取  $\alpha_1$  的特征向量  $a_1$  作为  $W_{1,r_1}$  的基底中元即可。当  $r_1 \geq 2$  时,如果把  $[a_1]$  作为 § 13 命题 33 中的  $W_1$ ,那末表示  $f_1$  的矩陣就成为

$$\begin{pmatrix} \alpha_1 & * \\ 0_{r_1-1,1} & F^{(1)} \end{pmatrix}$$

的形状,因此  $f_1$  的特征多项式显然是  $(X - \alpha_1) \varphi_{F^{(1)}}(X)$ , 另一方面它等于 (11.3), 因为  $r_1 \geq 2$ , 所以  $\varphi_{F^{(1)}}(X) = 0$  具有根  $X - \alpha_1$ , 由命题 40,  $\alpha_1$  是  $F^{(1)}$  的特征值, 于是  $\alpha_1$  的 (对于  $F^{(1)}$  的) 特征空间的维数大于零。因此由 § 13 命题 33 的系, 适当取  $V$  的基底, 那末  $f_1$  的矩陣就成为

$$\begin{pmatrix} \alpha_1 & * & * \\ 0 & \alpha_1 & * \\ 0_{r_1-2,2} & & F^{(2)} \end{pmatrix}$$

的形状, 所以不得不  $\dim W_{1,r_1} \geq 2$ 。假如  $r_1 \geq 3$ , 同样更进一步就能够得到  $\dim W_{1,r_1} \geq 3$ 。重复这个方法 (严密地, 由数学归纳法), 命题即得到証明。

**命题 42** 假设  $W_{i,r_i} = W_i$ , 那末  $W_1, \dots, W_k$  无关。

**証明** 由 § 4 定理 1, 証明  $x_1 + \dots + x_k = 0$ ,  $x_i \in W_i \Rightarrow x_i = 0$  即可。H. Weyl 曾用如下的巧妙的方法来証明。

假如根据 (14.3) 把  $1/\phi_i(X)$  分为部分分式,

$$\frac{1}{\phi_i(X)} = \frac{\phi^{(1)}(X)}{(X - \alpha_1)^{r_1}} + \dots + \frac{\phi^{(k)}(X)}{(X - \alpha_k)^{r_k}}. \quad (14.5)$$

命

$$\begin{aligned} \frac{\phi_i(X)}{(X - \alpha_i)^{r_i}} &= (X - \alpha_1)^{r_1} \dots (X - \alpha_{i-1})^{r_{i-1}} (X - \alpha_{i+1})^{r_{i+1}} \dots (X - \alpha_k)^{r_k} \\ &= \psi^{(i)}(X), \end{aligned} \quad (14.6)$$

$$\Phi^{(i)}(X)\Psi^{(i)}(X)=\Psi_i(X), \quad (14.7)$$

$$\Psi_i(f)=g_i\in\mathfrak{L}(V), \quad (14.8)$$

于是由 (14.5),

$$\Psi_1(x)+\cdots+\Psi_k(x)=1,$$

所以

$$g_1+\cdots+g_k=e_V \quad (V \text{ 的恒等映射}). \quad (14.9)$$

又假设  $x_i\in W_i$ , 因为  $(f-\alpha_i)^{r_i}(x_i)=0$ , 由 (14.6), (14.7), (14.8) 立即得到

$$i\neq j\Rightarrow g_j(x_i)=0. \quad (14.10)$$

于是考虑  $x_1+\cdots+x_k=0$ ,  $x_i\in W_i$ , 两边对于  $g_1$  的象, 根据 (14.10) 即得  $g_1(x_1)=0$ , 但由 (14.9), (14.10),  $g_1(x_1)=x_1$ , 因此  $x_1=0$ , 同样  $x_2=\cdots=x_k=0$ .

用上面结果能够证明下面的定理。

**定理 16** 假定  $f$  是  $n$  维向量空间  $V$  的线性变换, 它的特征值  $\alpha_1, \cdots, \alpha_k$  都在基础体  $K$  中, 这时如果  $f$  的特征多项式  $\Phi_f(X)$  因式分解为

$$\Phi_f(X)=(X-\alpha_1)^{r_1}\cdots(X-\alpha_k)^{r_k}$$

的形状,  $\text{Ker}(f-\alpha_i)^{r_i}=W_i$  ( $i=1, 2, \cdots, k$ ), 那末  $V=W_1\oplus\cdots\oplus W_k$ ,  $\dim W_i=r_i$ , 假如  $f|_{W_i}=f_i$ , 那末  $f_i$  的特征多项式是  $(X-\alpha_i)^{r_i}$ .

**证明** 由命题 42,  $W_1, \cdots, W_k$  是无关, 所以  $V\supset W_1+\cdots+W_k=W_1\oplus\cdots\oplus W_k$ . 由 §5 定理 5 的系 4 及命题 41,  $\dim(W_1\oplus\cdots\oplus W_k)=\sum\dim W_i\geqslant\sum r_i$ . 因此  $\dim V=n\geqslant\sum r_i$ . 另一方面, 由 (14.4),  $n=\sum r_i$ , 因此在命题 41 的结论中不等号不能成立. 又因为适当取  $W_i$  的基底, 表示  $f_i$  的矩阵能够成为  $\alpha_i$  恰好在主对角线上的  $r_i$  级三角型, 于是它的特征多项式是  $(X-\alpha_i)^{r_i}$ . 再因为  $\dim V=\dim\sum\oplus W_i$ , 所以

$$V=W_1\oplus\cdots\oplus W_k.$$

例5 命題 41 后面的“注意”事項可由上面的證明得知。

例6 用(14.8)定义的  $g_i$  是自  $V$  到  $W_i$  的射影 (§7 例4)。又  $f \circ g_i = f_i$ 。

于是由这定理及 §13 命題 34, 我們的問題 A 归結为  $f$  的特征多项式属于  $(X - \alpha)^r$  形状的情况。这时由于基底的选择, 显然表示  $f$  的矩陣能够成为三角型。問題 A 的最后解决让于下节。由上面的結果容易推得下面 Cayley-Hamilton 的重要定理。

**定理 17** (Cayley-Hamilton 定理) 假定  $F$  是任意方陣,  $\Phi_F(X)$  是它的特征多项式, 那末  $\Phi_F(F) = 0$ 。

例7 就例4的情形來說明 Cayley-Hamilton 定理。

$$[\text{解}] \quad F = \begin{pmatrix} 1 & 2 & 2 \\ 1 & -1 & 1 \\ 4 & -12 & 1 \end{pmatrix}, \quad \text{所以 } F^2 = \begin{pmatrix} 11 & -24 & 6 \\ 4 & -9 & 2 \\ -4 & 8 & -3 \end{pmatrix}.$$

$$\Phi_F(X) = \lambda^3 - X^2 + X - 1 = (X - 1)(X^2 + 1),$$

$$\text{因此 } \Phi_F(F) = (F - E)(F^2 + E)$$

$$= \begin{pmatrix} 0 & 2 & 2 \\ 1 & -2 & 1 \\ 4 & -12 & 0 \end{pmatrix} \begin{pmatrix} 12 & -24 & 6 \\ 4 & -8 & 2 \\ -4 & 8 & -2 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

为了証明 Cayley-Hamilton 定理, 首先証明下面两个引理。

**引理 3** 当  $\Psi(X)$  是  $X$  的任意多项式时, 如果

$$F = F_1 \oplus \cdots \oplus F_k,$$

$$\text{那末 } \Psi(F) = \Psi(F_1) \oplus \cdots \oplus \Psi(F_k).$$

**証明** 一般假定  $A$  与  $A'$ ,  $B$  与  $B'$ ,  $\dots$ ,  $L$  与  $L'$  分别是同級的方陣, 显然

$$(A \oplus B \oplus \cdots \oplus L) + (A' \oplus B' \oplus \cdots \oplus L') = (A + A') \oplus \cdots \oplus (L + L'),$$

$$\alpha(A \oplus B \oplus \cdots \oplus L) = \alpha A \oplus \alpha B \oplus \cdots \oplus \alpha L,$$

$$(A \oplus B \oplus \cdots \oplus L)(A' \oplus B' \oplus \cdots \oplus L') = AA' \oplus BB' \oplus \cdots \oplus LL'.$$

重复引用此事实, 即容易得到引理。

**引理 4** 假定  $F$  是象下面那样主对角綫上元素都是 0 的  $n$  級

三角型矩阵,

$$F = \begin{pmatrix} 0 & & * \\ & \ddots & \\ 0 & & 0 \end{pmatrix},$$

那末  $F^n = 0$ .

**证明** 由计算

$$F^2 = \begin{pmatrix} 0 & 0 & * \\ & \ddots & \\ 0 & & 0 \end{pmatrix}, F^3 = \begin{pmatrix} 0 & 0 & 0 & * \\ & \ddots & & \\ & 0 & \ddots & \\ & & & 0 \end{pmatrix}, \dots$$

所以  $F^n = 0$ .

象这样自乘若干回成为 0 的矩阵, 叫做**幂零**。一般, 对于环  $S$  中元  $x$ , 存在使  $x^n = 0$  的自然数  $n$  时,  $x$  叫做  $S$  的**幂零元**。

**Cayley-Hamilton 定理的证明** 证明  $\Phi_f(f) = 0$  即可。由定理 16, 分解

$$\Phi_f(X) = (X - \alpha_1)^{r_1} \cdots (X - \alpha_k)^{r_k},$$

适当取  $W_i = \text{Ker}(f - \alpha_i)^{r_i}$  的基底, 那末  $f|_{W_i} = f_i$  可以用矩阵

$$F_i^* = \begin{pmatrix} \alpha_i & & * \\ & \ddots & \\ 0 & & \alpha_i \end{pmatrix} \text{ 表示。因为 } V = W_1 \oplus W_2 \oplus \cdots \oplus W_k, \text{ 合并 } W_i \text{ 这}$$

$\xleftarrow{r_i}$

样的基底就得到  $V$  的基底, 由此,  $f$  可以用矩阵

$$F^* = F_1^* \oplus F_2^* \oplus \cdots \oplus F_k^*$$

表示。于是就这  $F^*$  来证明  $\Phi_f(F^*) = 0$  即可。

由引理 3,

$$\Phi_f(F^*) = \Phi_f(F_1^*) \oplus \Phi_f(F_2^*) \oplus \cdots \oplus \Phi_f(F_k^*).$$

在右边,譬如

$$\Phi_f(F_1^*) = (F_1^* - \alpha_1 E)^{r_1} \cdots (F_1^* - \alpha_k E)^{r_k},$$

因为

$$F_1^* - \alpha_1 E = \begin{pmatrix} 0 & & * \\ & \ddots & \\ 0 & & 0 \end{pmatrix},$$

$\xleftrightarrow{r_1}$

由引理 4,  $(F_1^* - \alpha_1 E)^{r_1} = 0$ . 因而  $\Phi_f(F_1^*) = 0$ . 同样  $\Phi_f(F_2^*) = 0$ ,  $\dots$ ,  $\Phi_f(F_k^*) = 0$ , 所以  $\Phi_f(F^*) = 0$ .

### § 15 Jordan 标准形

在 § 14 中已把 § 13 提出的問題 A 归結为  $f$  的特征多項式  $\Phi_f(X)$  是  $(X - \alpha)^n$ ,  $n = \dim V$  形状的情况。以下就此情况来解答問題 A.

由 § 14 命題 41 后面的注意 (参照定理 16 后面的例 5), 这时适当选取  $\varphi$ , 能够使  $F$  成为

$$\begin{pmatrix} \alpha & & * \\ & \ddots & \\ 0 & & \alpha \end{pmatrix}$$

形状, 因此由定理 17,  $(f - \alpha)^n = 0$ . 命  $f - \alpha = g$ , 那末  $g^n = 0$ . 即  $g$  是  $\mathfrak{L}(V)$  的幂零元。又适当选取  $\varphi$ , 因为表示  $g$  的矩陣为

$$\begin{pmatrix} 0 & & * \\ & \ddots & \\ 0 & & 0 \end{pmatrix},$$

所以  $\mathfrak{C}_g = \{0\}$ .

于是对于  $i = 0, 1, 2, \dots$ , 命

$$\text{Ker } g^i = V^{(i)}, \quad \dim V^{(i)} = d^{(i)} \quad (15.1)$$

(但  $g^0 = e_V$  (恒等映射)), 显然

$$V^{(0)} = \{0\} \subset V^{(1)} \subset V^{(2)} \subset \dots \subset V^{(n)} = V,$$

$$0 = d^{(0)} \leq d^{(1)} \leq d^{(2)} \leq \dots \leq d^{(n)} = n. \quad (15.2)$$

**命题 43** 在 (15.2) 中,

$$0 = d^{(0)} < d^{(1)}, \quad (15.3)$$

又对于某个自然数  $\mu$ , 假如

$$d^{(\mu)} = d^{(\mu+1)}, \quad (15.4)$$

那末

$$d^{(\mu+1)} = d^{(\mu+2)} = \dots = n. \quad (15.5)$$

**证明** (15.3) 意味着  $V^{(1)} = \text{Ker } g$  含有非 0 的向量, 因为由上面可知 0 是  $g$  的特征值, 所以这是显然的。

又 (15.4)  $\Rightarrow$  (15.5) 意味着 “ $V^{(\mu)} = V^{(\mu+1)} \Rightarrow V^{(\mu+1)} = V^{(\mu+2)}$ ”, 即假定 “ $g^{\mu+1}(x) = 0 \Rightarrow g^{\mu}(x) = 0$ , 那末  $g^{\mu+2}(y) = 0 \Rightarrow g^{(\mu+1)}(y) = 0$ ”, 这命  $x = g(y)$  即得。 (证毕)

设在数列  $d^{(0)}, d^{(1)}, \dots, d^{(n)}$  中使 (15.4) 成立的  $\mu$  的最小数是  $\nu$ , 由 (15.3),  $1 \leq \nu$  (当然  $\nu \leq n$ ). 于是

$$d^{(0)} = 0 < d^{(1)} < d^{(2)} < \dots < d^{(\nu)} = n = d^{(\nu+1)} = \dots,$$

$$V^{(0)} = \{0\} \subsetneq V^{(1)} \subsetneq V^{(2)} \subsetneq \dots \subsetneq V^{(\nu)} = V.$$

首先,  $\nu = 1$  的情形是简单的, 这时因为

$$V^{(1)} = \text{Ker } g = \text{Ker } (f - \alpha) = V,$$

所以  $g = 0, f = \alpha$ . 因此  $V$  的基底不论怎样选取, 表示  $f$  的矩阵是  $\alpha E$ .

以下考虑  $\nu \geq 2$  的情形, 这时命

$$d^{(i)} - d^{(i-1)} = e^{(i)}, \quad i = 1, 2, \dots, \nu. \quad (15.6)$$

因为  $d^{(0)} = 0, d^{(i-1)} < d^{(i)}, d^{(\nu)} = n$ , 所以

$$e^{(1)} = d^{(1)}, \quad e^{(i)} > 0, \quad \sum_{i=1}^{\nu} e^{(i)} = n.$$

在  $V^{(i)}$  中能够取  $e^{(i)}$  个关于  $\text{mod } V^{(i-1)}$  无关的向量

$$x^{(i,1)}, \dots, x^{(i,e^{(i)})}, \quad (15.7)$$

把它们合并起来, 显然就得到  $V$  的基底。

为了解答我們的问题 A, 在  $V$  中就选取那样的基底, 对于它的坐标系假定是  $\varphi$ , 但是在选取那基底时, 还須注意下面的事实。

**命题 44** 当  $1 \leq i \leq \nu - 2$  时, 假如 (15.7) 是  $V^{(i)}$  中关于  $\text{mod } V^{(i-1)}$  无关的向量, 那末

$$g(x^{(i,1)}), \dots, g(x^{(i,e^{(i)})}) \quad (15.7')$$

就是  $V^{(i-1)}$  中关于  $\text{mod } V^{(i-2)}$  无关的向量。因此  $e^{(i)} \leq e^{(i-1)}$ 。

**証明** (15.7') 的向量是  $V^{(i-1)}$  中元意味着  $g^{(i-1)}(g(x^{(i,1)})), \dots, g^{(i-1)}(g(x^{(i,e^{(i)})}))$  都是 0, 这由  $x^{(i,1)}, \dots, x^{(i,e^{(i)})} \in V^{(i)}$ , 即  $g^i(x^{(i,1)}) = 0$  可以明白。又 (15.7') 的向量关于  $\text{mod } V^{(i-2)}$  无关就意味着

$$\lambda_1 g(x^{(i,1)}) + \dots + \lambda_{e^{(i)}} g(x^{(i,e^{(i)})}) \in V^{(i-2)} \Rightarrow \lambda_1 = \dots = \lambda_{e^{(i)}} = 0,$$

这由 (15.7) 的向量关于  $\text{mod } V^{(i-1)}$  无关立即明白。 (証毕)

今对于  $i$  的某个給定值, (15.7) 的向量用  $(\eta)_i$  表示, 那末合并

$$(\eta)_1, (\eta)_2, \dots, (\eta)_{\nu-1}, (\eta)_\nu$$

就成为  $V$  的基底, 但是引用命题 44, 它可以象下面那样来选取。

首先, 任意选  $(\eta)_\nu: x^{(\nu,1)}, \dots, x^{(\nu,e^{(\nu)})}$ , 为了简单, 它們用  $x^{(1)}, \dots, x^{(e^{(\nu)})}$  表示。

由命题 44, 这时能够选取

$$g(x^{(1)}), \dots, g(x^{(e^{(\nu)})})$$

作为  $(\eta)_{\nu-1}$  的一部分 (現在我們假定  $\nu \geq 2$ )。假如  $e^{(\nu)} = e^{(\nu-1)}$ , 那末它就是  $(\eta)_{\nu-1}$  的全部。不拘怎样, 取它作为  $(\eta)_{\nu-1}$  的一部 (或全部), 当  $e^{(\nu)} < e^{(\nu-1)}$  时, 任意附加  $V^{(\nu-1)}$  中  $e^{(\nu-1)} - e^{(\nu)}$  个关于  $\text{mod } V^{(\nu-2)}$  无关的向量  $x^{(e^{(\nu)}+1)}, \dots, x^{(e^{(\nu-1)})}$ , 使之成为  $(\eta)_{\nu-1}$ 。更設  $\nu \geq 3$ , 考虑

$$g^2(x^{(1)}), \dots, g^2(x^{(e^{(\nu)})}), g(x^{(e^{(\nu)}+1)}), \dots, g(x^{(e^{(\nu-1)})}),$$

因為它們是  $V^{(\nu-2)}$  中关于  $\text{mod } V^{(\nu-3)}$  无关的向量, 所以它們成为  $(\eta)_{\nu-2}$  的一部分 (或全部)。这样, 繼續  $\nu$  回就得到  $\nu e^{(\nu)}$  个向量

$$x^{(i)}, g(x^{(i)}), \dots, g^{v-1}(x^{(i)}), \quad i=1, \dots, e^{(v)}, \quad (15.8)$$

$(v-1)(e^{(v-1)}-e^{(v)})$  个向量

$$x^{(j)}, g(x^{(j)}), \dots, g^{v-2}(x^{(j)}), \quad j=e^{(v)}+1, \dots, e^{(v-1)} \quad (15.9)$$

等等, 把它们合并后就得

$$ve^{(v)} + (v-1)(e^{(v-1)}-e^{(v)}) + \dots + 1(e^{(1)}-e^{(v)}) = \sum e^{(i)} = n$$

个无关向量, 即  $V$  的基底。

于是用 (15.8) 中  $v$  个向量生成的子空间  $[x^{(i)}, \dots, g^{v-1}(x^{(i)})] = W^{(i)}$  由  $g^v=0$  容易得知是  $g$  的 (因而又是  $f=g+\alpha$  的) 不变子空间。  $V$  显然是  $e^{(v)}$  个  $v$  维不变子空间  $W^{(1)}, \dots, W^{(e^{(v)})}$ ;  $(e^{(v-1)}-e^{(v)})(\geq 0)$  个  $(v-1)$  维不变子空间  $W^{(e^{(v)}+1)}, \dots, W^{(e^{(v-1)})}$  等等的直和。假如对于  $W^{(i)}$  的基底表示  $g|W^{(i)}=g^{(i)}, f|W^{(i)}=f^{(i)}$  的矩阵分别是  $G^{(i)}, F^{(i)}$ , 那末  $g, f$  可以分别用矩阵  $G^{(1)} \oplus G^{(2)} \oplus \dots, F^{(1)} \oplus F^{(2)} \oplus \dots$  来表示。

现在就  $i=1$  来考虑,  $W^{(1)}$  的基底仍旧取 (15.8) 的向量, 但是改变番号, 命

$$a_1 = g^{v-1}(x^{(1)}), \quad a_2 = g^{v-2}(x^{(1)}), \quad \dots, \quad a_v = x^{(1)}. \quad (15.10)$$

取此作为基底, 那末表示  $g^{(1)}$  的矩阵显然是

$$G^{(1)} = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \\ 0 & 0 & 0 & \dots & 0 \end{pmatrix} \quad \begin{matrix} \uparrow \\ \vdots \\ \downarrow \end{matrix} \quad \begin{matrix} v \\ \vdots \\ v \end{matrix}$$

的形状。因此对于同样基底来表示  $f|W^{(1)}=f^{(1)}=g^{(1)}+\alpha$ , 就得到

$$F^{(1)} = \begin{pmatrix} \alpha & 1 & 0 & \dots & 0 \\ 0 & \alpha & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \\ 0 & 0 & 0 & \dots & \alpha \end{pmatrix} \quad \begin{matrix} \uparrow \\ \vdots \\ \downarrow \end{matrix} \quad \begin{matrix} v \\ \vdots \\ v \end{matrix} \quad (15.11)$$



形状的矩陣。这右边的矩陣用  $J(\alpha, \nu)$  表示(于是  $G^{(1)} = J(0, \nu)$ )。当  $e^{(\nu-1)} > e^{(\nu)}$  时, 对于  $e^{(\nu)} + 1 \leq j \leq e^{(\nu-1)}$  的  $j$  作同样的考虑, 由 (15.9), 容易得知  $f|W^{(j)} = f^{(j)}$  是用矩陣  $J(\alpha, \nu-1)$  表示。

綜合以上事实, 在我們的假定下, 得到下面解答問題 A 的定理。

**定理 18** 假定  $f$  是  $n$  維向量空間  $V$  的綫型变换, 它的特征多項式  $\Phi_f(X)$  是  $(X-\alpha)^n$  的形状, 那末适当取  $V$  的坐标系  $\varphi$ , 就能够用下面形状的矩陣表示  $f$ ,

$$\underbrace{J(\alpha, \nu) + \cdots + J(\alpha, \nu)}_{e^{(\nu)} \uparrow} + \underbrace{J(\alpha, \nu-1) + \cdots + J(\alpha, \nu-1)}_{(e^{(\nu-1)} - e^{(\nu)}) \uparrow} + \cdots, \quad (15.12)$$

这里  $J(\alpha, \nu)$  是用 (15.11) 定义的矩陣,  $e^{(i)}$  是用 (15.1), (15.6) 定义的自然数,

$$\begin{aligned} e^{(i)} &= d^{(i)} - d^{(i-1)} = \dim \operatorname{Ker}(f-\alpha)^i - \dim \operatorname{Ker}(f-\alpha)^{i-1} \\ &= d(f-\alpha)^i - d(f-\alpha)^{i-1} = r(f-\alpha)^{i-1} - r(f-\alpha)^i. \end{aligned}$$

( $d$  是退化次数,  $r$  是秩)。因此

$$0 \leq e^{(\nu)} \leq e^{(\nu-1)} \leq \cdots \leq e^{(1)} = \dim \operatorname{Ker}(f-\alpha).$$

**系** 用上面的記法,  $(f-\alpha)^\nu = 0$ .

$\nu$  叫做  $f$  (或表示它的矩陣) 的**簡約次数** (这概念在这里是就特征多項式为  $(X-\alpha)^n$  形状的变换(或矩陣)来定义的)。

(15.12) 形状的矩陣一般用  $J(\alpha)$  表示, ( $J(\alpha, \nu)$  是由  $\alpha$  与  $\nu$  确定的  $\nu$  級矩陣, 但  $J(\alpha)$  当然不能作为由  $\alpha$  确定的矩陣。  $J(\alpha)$  只是表示“矩陣的形状”)。这时,  $J(\alpha_1) \oplus J(\alpha_2) \oplus \cdots \oplus J(\alpha_k)$  形状的矩陣叫做 **Jordan 标准形**。

由定理 16, 18, 得到下面关于問題 A 的决定結果。

**定理 19** 假定  $f$  是向量空間  $V$  的綫性变换, 它的特征多項式是

$$\Phi_f(X) = (X - \alpha_1)^{r_1} \cdots (X - \alpha_k)^{r_k}, \quad (15.13)$$

这时,适当取  $V$  的坐标系  $\varphi$ , 则  $f$  能够用

$$J(\alpha_1) \oplus \cdots \oplus J(\alpha_k) \quad (15.14)$$

形状的 Jordan 标准形矩阵表示。

**证明** 由定理 16, 自 (15.13) 命  $\text{Ker}(f - \alpha_i)^{r_i} = W_i$ , 那末  $V$  直和分解为  $V = W_1 \oplus \cdots \oplus W_k$ ,  $\dim W_i = r_i$ , 假定  $f|W_i = f_i$ , 那末  $f_i$  的特征多项式为  $(X - \alpha_i)^{r_i}$ . 由定理 18, 对于  $W_i$  取适当基底,  $f_i$  能够用  $J(\alpha_i)$  形状的矩阵表示。把它们合并后所成的  $V$  的基底, 由它确定的坐标系作为  $\varphi$  即可。

**系 1** 假定  $f_i$  的简约次数是  $\nu_i$ ,

$$\Psi_f(X) = (X - \alpha_1)^{\nu_1} \cdots (X - \alpha_k)^{\nu_k},$$

那末  $\Psi_f(f) = 0$ .

$\nu_i$  叫做  $f$  对于特征值  $\alpha_i$  的简约次数,  $\Psi_f(X)$  的次数  $\nu_1 + \cdots + \nu_k$  叫做  $f$  的简约次数。

**系 2** 当  $n$  级方阵  $F$  已给定时, 取适当的  $n$  级正则矩阵  $P$  能够使得  $PF P^{-1}$  成为 Jordan 标准形。

**注意** 上面是取 (15.10) 作为  $W^{(1)}$  的基底, 假如取与 (15.8) 同样的顺序 (改变 (15.10) 的记号) 附加番号成为

$$a_1 = x^{(1)}, a_2 = g(x^{(1)}), \cdots, a_\nu = g^{\nu-1}(x^{(1)}),$$

以这作为基底, 那末所得到的表示  $f^{(1)}$  的矩阵是 (15.11) 中  $F^{(1)}$  的  ${}^t F^{(1)}$  (矩阵的形状由第 2 三角型变为第 1 三角型)。这样就得到上述“Jordan 标准形矩阵”的转置矩阵, 有时也叫这种形状为“Jordan 标准形”。

**例 1**  $f$  能够用对角线型矩阵表示的必要充分条件是  $f$  对于各个特征值的简约次数都是 1, 即  $\nu_1 = \nu_2 = \cdots = \nu_k = 1$ . 特别,

$$\Phi_f(X) = (X - \alpha_1) \cdots (X - \alpha_n), \quad i \neq j \Rightarrow \alpha_i \neq \alpha_j$$

时,  $f$  能够用对角线型矩阵表示。

[解] 假定  $\Phi_f(X) = (X - \alpha_1)^{r_1} (X - \alpha_2)^{r_2} \cdots (X - \alpha_k)^{r_k}$ ,

命  $W_i = \text{Ker}(f - \alpha_i)^{r_i}$ ,  $V = W_1 \oplus W_2 \oplus \cdots \oplus W_k$ ,  $\dim W_i = r_i$ ,

$f_i = f|W_i$  的简约次数是  $\nu_i$ . 如果  $\nu_i = 1$ , 象命题 44 后面所述的那样,  $f_i$  的

矩陣能够用  $F_i = \alpha_i E_{r_i}$  表示, 所以  $f$  能够用

$$F = \alpha_1 E_{r_1} \oplus \alpha_2 E_{r_2} \oplus \cdots \oplus \alpha_k E_{r_k}$$

表示。它是对角綫型矩陣。

反之, 如果  $f$  能够用这样的对角綫型矩陣表示, 則显然对于各个特征值  $\alpha_i$  的簡約次数  $\nu_i$  都是 1。

**例 2** 就 § 14 例 4, 例 7 中提出的

$$F = \begin{pmatrix} 1 & 2 & 2 \\ 1 & -1 & 1 \\ 4 & 12 & 1 \end{pmatrix}$$

来解答問題 A。

[解] 象在 § 14 例 4 中那样,  $\varphi_f(X) = (X-1)(X-i)(X+i)$ , 并且  $W_1 = \text{Ker}(F-E) = W(1)$ ,  $W_2 = \text{Ker}(F-iE) = W(i)$ ,  $W_3 = \text{Ker}(F+iE) = W(-i)$  的基底能够分別选取

$$\alpha_1 = \begin{pmatrix} 3 \\ 1 \\ -1 \end{pmatrix}, \quad \alpha_2 = \begin{pmatrix} 4+2i \\ 1+i \\ -4 \end{pmatrix}, \quad \alpha_3 = \begin{pmatrix} 4-2i \\ 1-i \\ -4 \end{pmatrix}.$$

以  $\{\alpha_1, \alpha_2, \alpha_3\}$  作为  $V$  的基底, 假如把坐标变为由它所确定的坐标, 那末  $F$  应该用矩陣  $F_0$  来表示,

$$F_0 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & i & 0 \\ 0 & 0 & -i \end{pmatrix}.$$

假設坐标变换的矩陣是  $P$ , 显然

$$P^{-1} = \begin{pmatrix} 3 & 4+2i & 4-2i \\ 1 & 1+i & 1-i \\ -1 & -4 & -4 \end{pmatrix},$$

因此

$$P = (P^{-1})^{-1} = \begin{pmatrix} 2 & -4 & 1 \\ \frac{-1+3i}{4} & \frac{1-4i}{2} & \frac{-1+i}{4} \\ \frac{-1}{4} & \frac{1+4i}{2} & \frac{-1-i}{4} \end{pmatrix}.$$

由实际計算得

$$\begin{aligned}
 P^{-1}P^{-1} &= \begin{pmatrix} 2 & -4 & 1 \\ \frac{-1+3i}{4} & \frac{1-4i}{2} & \frac{-1+i}{4} \\ \frac{-1-3i}{4} & \frac{1+4i}{2} & \frac{-1-i}{4} \end{pmatrix} \begin{pmatrix} 1 & 2 & 2 \\ 1 & -1 & 1 \\ 4 & -12 & 1 \end{pmatrix} \begin{pmatrix} 3 & 4+2i & 4-2i \\ 1 & 1+i & 1-i \\ -1 & -4 & -4 \end{pmatrix} \\
 &= \begin{pmatrix} 2 & -4 & 1 \\ \frac{-3-i}{4} & \frac{4+i}{2} & \frac{-1-i}{4} \\ \frac{-3+i}{4} & \frac{4-i}{2} & \frac{-1+i}{4} \end{pmatrix} \begin{pmatrix} 3 & 4+2i & 4-2i \\ 1 & 1+i & 1-i \\ -1 & -4 & -4 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & i & 0 \\ 0 & 0 & -i \end{pmatrix}.
 \end{aligned}$$

**例 3** 假设  $K = \mathbb{C}$ , 试将

$$F = \begin{pmatrix} -4 & 9 & -4 \\ -9 & 18 & -8 \\ -15 & 29 & -13 \end{pmatrix}$$

变为 Jordan 标准形。

[解] 求出特征多项式

$$\Phi_F(X) = X^3 - X^2 - X + 1 = (X-1)^2(X+1),$$

命

$$W_1 = \text{Ker}(F-E)^2 \supset W'_1 = \text{Ker}(F-E), \quad W_2 = \text{Ker}(F+E).$$

解

$$(F-E)x = \begin{pmatrix} -5 & 9 & -4 \\ -9 & 17 & -8 \\ -15 & 29 & -14 \end{pmatrix} x = 0, \text{ 得 } W'_1 = \left\{ \lambda \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}; \lambda \in \mathbb{C} \right\}.$$

解

$$(F-E)^2 x = \begin{pmatrix} 4 & -8 & 4 \\ 12 & -24 & 12 \\ 24 & -48 & 24 \end{pmatrix} x = 0, \text{ 得 } W_1 = \left\{ \lambda \begin{pmatrix} 2 \\ 1 \\ 0 \end{pmatrix} + \mu \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}; \lambda, \mu \in \mathbb{C} \right\}.$$

解

$$(F+E)x = \begin{pmatrix} -3 & 9 & -4 \\ -9 & 19 & -8 \\ -15 & 29 & -12 \end{pmatrix} x = 0, \text{ 得 } W_2 = \left\{ \lambda \begin{pmatrix} 1 \\ 3 \\ 6 \end{pmatrix}; \lambda \in \mathbb{C} \right\}.$$

兹求作以 Jordan 标准形表示  $F$  的基底。首先取  $W_1$  中对于  $\text{mod } W'_1$  无

关的向量  $a_2 = \begin{pmatrix} 2 \\ 1 \\ 0 \end{pmatrix}$ , 次取  $a_1 = (F-E)a_2 = \begin{pmatrix} -5 & 9 & -4 \\ -9 & 17 & -8 \\ -15 & 29 & -14 \end{pmatrix} \begin{pmatrix} 2 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} -1 \\ -1 \\ -1 \end{pmatrix}$  作

为  $W_1$  的基底。因此  $W_1 = \left[ \begin{pmatrix} -1 \\ -1 \\ 1 \end{pmatrix}, \begin{pmatrix} 2 \\ 1 \\ 0 \end{pmatrix} \right]$ 。再取  $a_3 = \begin{pmatrix} 1 \\ 3 \\ 6 \end{pmatrix}$  作为  $W_2$  的基底，

于是  $F$  应该用 Jordan 标准形  $F_0 = \left( \begin{array}{cc|c} 1 & 1 & 0 \\ 0 & 1 & 0 \\ \hline 0 & 0 & -1 \end{array} \right)$  表示。

坐标变换的矩阵  $P$ ，由

$$P^{-1} = \begin{pmatrix} -1 & 2 & 1 \\ -1 & 1 & 3 \\ -1 & 0 & 6 \end{pmatrix}, \quad \text{则 } P = \begin{pmatrix} 6 & -12 & 5 \\ 3 & -5 & 2 \\ 1 & -2 & 1 \end{pmatrix},$$

实际计算得

$$\begin{aligned} PFP^{-1} &= \begin{pmatrix} 6 & -12 & 5 \\ 3 & -5 & 2 \\ 1 & -2 & 1 \end{pmatrix} \begin{pmatrix} -4 & 9 & -4 \\ -9 & 18 & -8 \\ -15 & 29 & -13 \end{pmatrix} \begin{pmatrix} -1 & 2 & 1 \\ -1 & 1 & 3 \\ -1 & 0 & 6 \end{pmatrix} \\ &= \begin{pmatrix} 6 & -12 & 5 \\ 3 & -5 & 2 \\ 1 & -2 & 1 \end{pmatrix} \begin{pmatrix} -1 & 1 & -1 \\ -1 & 0 & -3 \\ -1 & -1 & -6 \end{pmatrix} \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}. \end{aligned}$$

## § 16 Euclid 空间

我们在 § 1 中说明了，对于“在力学上使用的向量”， $A, B, C$  三个事实都成立。在 § 3 中，根据重述的  $A, B, C$  定义了作为代数系的“向量空间”，这样一直论述到现在。但是对于“在力学上使用的向量”，能够成立的事实很多，不仅仅是  $A, B, C$ （及自它导出的事实）而已。从这些事实之中，我们所以特别抽出  $A, B, C$  是因为只由它们就能够导出其他各种事实，正象直到现在所看到的那样。又满足  $A, B, C$  的“向量空间”，出现在数学的各部门中。 $A, B, C$  确是数学家根据经验与智慧所发现的“好公理”。

下面讨论“在力学上使用的向量”的另一有用性质（不含于

$A, B, O$ ), 这就是向量  $x, y$  間所定义的内积  $xy$ . 下面关于内积的一些性质, 想讀者已經知道。

(i) 假定对于空間直交坐标,

$$x = (x_1, x_2, x_3),$$

$$y = (y_1, y_2, y_3),$$

那末  $xy = x_1y_1 + x_2y_2 + x_3y_3$ .

(ii)  $xy = yx$ ,

$$(x_1 + x_2)y = x_1y + x_2y,$$

对于  $\alpha \in \mathbf{R}$ , 有  $(\alpha x)y = \alpha(xy)$ .

(iii) 假定  $xx = x^2$ , 那末  $x^2 = x_1^2 + x_2^2 + x_3^2 \geq 0$ ,  
 $|x| = \sqrt{x^2}$  是向量  $x$  的长, 并且  $x = 0 \Leftrightarrow |x| = 0$ .

(iv) 假定  $x, y$  之間的夹角是  $\theta$ , 那末

$$xy = |x| \cdot |y| \cos \theta.$$

特別,  $x \perp y \Rightarrow xy = 0$ .

把以上作为模型, 当  $\mathbf{R}$  上向量空間  $V$  满足下面的条件时, 我們叫  $V$  做 Euclid 的。Euclid 向量空間叫做一般 Euclid 空間, 有限維的一般 Euclid 空間叫做 Euclid 空間。

E1. 对于  $x, y \in V$ , 有  $\mathbf{R}$  中元  $xy$  与之对应,  $xy$  叫做  $x, y$  的内积。

E2.  $xy = yx$ .

E3.  $(x_1 + x_2)y = x_1y + x_2y$ .

E4. 对于任意  $\alpha \in \mathbf{R}$ ,  $(\alpha x)y = \alpha(xy)$ .

E5.  $xx = x^2 \geq 0$ ,  $x^2 = 0 \Leftrightarrow x = 0$ .

例 1 把  $y$  固定, 假定  $f(x) = xy$ , 那末  $f \in \mathfrak{L}(V, \mathbf{R})$ , 特別,

$$0 \cdot y = 0.$$

把  $x$  固定, 假定  $g(y) = xy$ , 那末  $g \in \mathfrak{L}(V, \mathbf{R})$ , 特別,

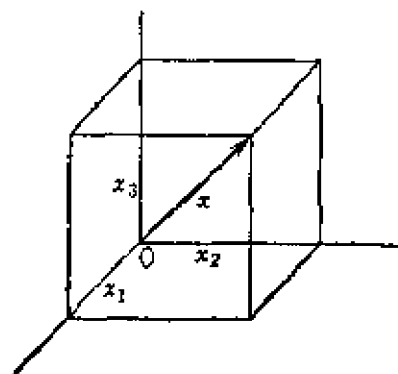


图 16.1

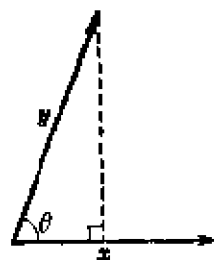


图 16.2

$$x \cdot 0 = 0,$$

例2 当  $V$  是  $R$  上  $n$  維向量空間时, 固定  $V$  的坐标系  $\varphi$ , 对于

$$\varphi(x) = \begin{pmatrix} \xi_1 \\ \vdots \\ \xi_n \end{pmatrix}, \quad \varphi(y) = \begin{pmatrix} \eta_1 \\ \vdots \\ \eta_n \end{pmatrix},$$

命  $xy = {}^t\varphi(x) \varphi(y) = \sum_{i=1}^n \xi_i \eta_i$ , 那末  $V$  成为 Euclid 的。

特別,  $R^n$  是根据  $xy = {}^t x \cdot y$  形成的 Euclid 空間。

例3 假定  $\alpha, \beta \in R$ , 区間  $[\alpha, \beta] = \Delta$ , 对于  $\mathfrak{E}(\Delta, R)$  (§3, 例10) 中元  $f, g, \dots$ , 規定

$$fg = \int_{\alpha}^{\beta} f(x)g(x)dx,$$

那末  $\mathfrak{E}(\Delta, R)$  成为 Euclid 空間。

例4 因为由 E 4,  $x^2 \geq 0$ , 所以  $\sqrt{x^2} \in R$ ,  $\sqrt{x^2} = |x|$  叫做  $x$  的长,

$$|\alpha x| = |\alpha| \cdot |x| \quad (\text{由 E 2, E 3}),$$

$$|x| = 0 \Leftrightarrow x = 0 \quad (\text{由 E 4}).$$

一般 Euclid 空間中长是 1 的元叫做单位向量。

以后如不預先声明,  $V$  作为一般 Euclid 空間,  $x, y, \dots$  表示它的元。

**命题 45**  $(xy)^2 \leq x^2 y^2$  (Cauchy-Schwarz 不等式)

**証明** 对于任意  $\xi \in R$ ,

$$0 \leq (\xi x + y)^2 = \xi^2 x^2 + 2\xi(xy) + y^2.$$

右边是  $\xi$  的二次三項式, 因为它的符号一定, 所以判別式不得不  $\leq 0$ , 即

$$(xy)^2 - x^2 y^2 \leq 0.$$

例 5①  $x \neq 0, |x||y| = xy \Rightarrow y = \alpha x, \alpha \geq 0$ .

① 假如  $(xy)^2 - x^2 y^2 = 0$ , 即  $(xy)^2 = x^2 y^2$ . 这就是說二次三項式  $\xi^2 x^2 + 2\xi(xy) + y^2$  的判別式  $= 0$ , 因此它有一个实根  $\xi_0 = -\frac{xy}{x^2}$ . 于是  $(\xi_0 x + y)^2 = 0$ , 由 E 5,  $\xi_0 x + y = 0$ , 所以  $y = -\xi_0 x$ . 因为  $x^2 > 0, |x| \geq 0, |y| \geq 0$ , 当  $|x| \cdot |y| = xy$  时,  $xy > 0$ , 因此  $\xi_0 < 0$ . 当  $|x| \cdot |y| = -xy$  时,  $xy < 0$ , 因此  $\xi_0 > 0$ . 令  $\alpha = -\xi_0$ , 即得  $y = \alpha x$ . ——譯者注

$$x \neq 0, |x| |y| = -xy \Rightarrow y = \alpha x, \alpha \leq 0.$$

例 6 当  $x \neq 0, y \neq 0$  时,  $\left| \frac{xy}{|x| \cdot |y|} \right| \leq 1$ .

are  $\cos \frac{xy}{|x| \cdot |y|} = \theta$  ( $0 \leq \theta \leq \pi$ ) 叫做  $x, y$  之間的角。

当  $x, y$  之間的角  $\theta = \frac{\pi}{2}$  即  $xy = 0$  时,  $x, y$  叫做**垂直或直交**, 写成  $x \perp y$ . 当  $x = 0$  或  $y = 0$  时, 总是  $xy = 0$ . 这时也叫  $x, y$  垂直。

**命题 46**  $|x+y| \leq |x| + |y|$ .

**証明**  $(x+y)^2 = x^2 + 2(xy) + y^2 \leq |x|^2 + 2|x||y| + |y|^2 = (|x| + |y|)^2$ . 取两边非負的平方根即得。

**系 1**  $|x-y| \geq |x| \sim |y|$ . ( $\sim$  表示差)。

**系 2**  $|x-y| + |y-z| \geq |x-z|$ .

**注意** 一般, 在由元  $x, y, z, \dots$  形成的集合  $S$  中, 假如对于任意两元  $x, y$ , 有叫做  $x, y$  之間的距离  $\rho(x, y)$  的非負实数与之对应, 并且

$$\rho(x, y) = 0 \Leftrightarrow x = y,$$

$$\rho(x, y) = \rho(y, x),$$

$$\rho(x, y) + \rho(y, z) \geq \rho(x, z).$$

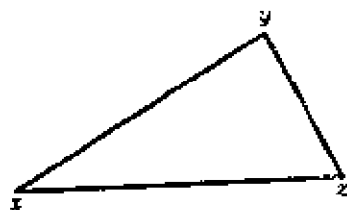


图 16.8

这时  $S$  叫做以  $\rho$  作为距离的**距离空間**。在一般 Euclid 空間  $V$  中, 假如  $|x-y| = \rho(x, y)$ , 那末  $V$  成为距离空間。

假定在  $V$  中有元  $x$  及子空間  $W$ , 如果  $x$  与  $W$  中任意元垂直, 那末  $x$  与  $W$  叫做**垂直或直交**, 写成  $x \perp W$ . 对于  $V$  的两个子空間  $W_1, W_2$ , 如果  $W_1$  中任意元  $x_1$  与  $W_2$  中任意元  $x_2$  恒垂直, 那末  $W_1, W_2$  叫做**垂直或直交**, 写成  $W_1 \perp W_2$ .

例 7  $W_1 \perp W_2$

$$\Leftrightarrow W_1 \text{ 中任意元 } x_1 \text{ 垂直于 } W_2,$$

$$\Leftrightarrow W_2 \text{ 中任意元 } x_2 \text{ 垂直于 } W_1.$$

① 因为  $(x-y)^2 = x^2 - 2(xy) + y^2 \geq x^2 - 2|x| \cdot |y| + y^2 = (|x| - |y|)^2$ , 所以  $|x-y| \geq |x| \sim |y|$ . ——譯者注



**例 8** 假定  $V$  有子空間  $W$ , 那末  $W' = \{y; y \perp W\}$  成为  $V$  中垂直于  $W$  的子空間。

例 8 中的子空間  $W'$  叫做  $W$  的直交补空間, 用  $W^\perp$  表示。

**命題 47** 假定  $\{x_1, x_2, \dots, x_k\}$  是  $V$  的  $k$  維子空間  $W$  的基底, 那末  $y \in V$  垂直于  $W$  的必要充分条件是  $x_i \perp y (i=1, 2, \dots, k)$ 。

**証明**  $W \perp y \Rightarrow x_i \perp y (i=1, 2, \dots, k)$  是明显的。

反之, 假如  $x_i \perp y (i=1, 2, \dots, k)$ . 因为  $W$  中任意元  $x$  能够表为  $x = \lambda_1 x_1 + \dots + \lambda_k x_k (\lambda_i \in R)$ , 所以  $xy = (\lambda_1 x_1 + \dots + \lambda_k x_k)y = \lambda_1(x_1 y) + \dots + \lambda_k(x_k y) = 0$ . 于是  $x \perp y$ . 因而  $W \perp y$ .

对于  $V$  的  $k$  个子空間  $W_1, W_2, \dots, W_k$ , 假如  $i \neq j$  时  $W_i \perp W_j$ , 那末  $W_1, W_2, \dots, W_k$  叫做直交系。又对于  $V$  中  $k$  个任意非零元  $a_1, a_2, \dots, a_k$ , 假如  $[a_1], [a_2], \dots, [a_k]$  是直交系, 那末  $a_1, a_2, \dots, a_k$  叫做直交系。

**命題 48** 假定  $W_1, W_2, \dots, W_k$  是直交系, 那末它們无关。

**証明** 假設  $x_i \in W_i (i=1, 2, \dots, k)$ , 如果  $x_1 + x_2 + \dots + x_k = 0$ , 那末  $0 = x_i(x_1 + x_2 + \dots + x_k) = x_i^2$ , 于是  $x_i = 0 (i=1, 2, \dots, k)$ , 所以  $W_1, W_2, \dots, W_k$  无关。

**系 1** 假定  $a_1, a_2, \dots, a_k$  是直交系, 那末它們綫性无关。

**系 2**  $n$  維 Euclid 空間  $V$  中  $n$  个元假如成为直交系, 那末它們就是  $V$  的基底。

由单位向量形成的直交系叫做正規直交系。正規直交系成为 Euclid 空間的基底时, 叫做正規直交基底或完全正規直交系。

**定理 20** 設  $V$  是  $n$  維 Euclid 空間,  $\{a_1, a_2, \dots, a_n\}$  是  $V$  的一个基底, 如果

$$b_1 = a_1, \quad e_1 = \frac{b_1}{|b_1|},$$

$$b_k = a_k - \sum_{i=1}^{k-1} (e_i, a_k) e_i, \quad e_k = \frac{b_k}{|b_k|} \quad (k=2, 3, \dots, n),$$

那末  $\{e_1, e_2, \dots, e_n\}$  是  $V$  的正規直交基底。

**証明** 显然  $\{e_1, e_2, \dots, e_n\}$  中都是单位向量。又当  $j < k$  时,

$$e_j b_k = e_j a_k - \sum_{i=1}^{k-1} (e_i a_k) e_j e_i = e_j a_k - e_j a_k = 0, \text{ 所以 } e_j e_k = 0.$$

于是  $\{e_1, e_2, \dots, e_n\}$  是正規直交系。因此成为正規直交基底。

**注意** 这样自 Euclid 空間  $V$  的任意基底作出正規直交基底的方法叫做 E. Schmidt 方法。

**系** Euclid 空間有正規直交基底。

Euclid 空間中由正規直交基底确定的坐标叫做直交坐标。

**定理 21** 假定  $W$  是一般 Euclid 空間  $V$  的有限維子空間, 那末

$$V = W \oplus W^\perp.$$

**証明** 因为  $W$  与  $W^\perp$  无关, 所以只要表明  $V = W + W^\perp$  即可。假定  $\{e_1, e_2, \dots, e_k\}$  是  $W$  的正規直交基底, 对于  $x \in V$ , 命

$$x' = \sum_{i=1}^k (e_i x) e_i, \quad x'' = x - x',$$

那末

$$x = x' + x'', \quad x' \in W,$$

又由  $e_i x'' = 0 (i=1, \dots, k)$ , 所以  $x'' \perp W$ , 因此  $V = W + W^\perp$ . (証毕)

由于上面的直和分解  $V = W \oplus W^\perp$ ,  $V$  到  $W$  上的射影  $P_W$  叫做到  $W$  上的正射影。对于一般 Euclid 空間  $V$ , 今后如无預先声明, 只写  $P_W$  就表示  $W$  是  $V$  的有限維子空間,  $P_W$  是到  $W$  上的正射影。

当  $a \in V, a \neq 0$  时, 把  $P_{[a]}$  单写成  $P_a$  叫做到  $a$  上的正射影。显然  $P_a(x) = (ax)a/|a|^2$  ①。

① 命  $W = [a], V = W + W^\perp, x = x' + x'', x' \in [a], x'' \in W^\perp$ , 于是  $x = \lambda a + x''$ . 因此  $ax = \lambda a^2, (ax)a = \lambda a^2 \cdot a$ , 所以  $\frac{(ax)a}{|a|^2} = \lambda a = x' = P_a(x)$ . ——譯者注

**例 9** 假定  $a_1, a_2, \dots, a_k$  是任意直交系。对于  $x \in V$ , 如果  $P_{a_i}(x) = x_i$ , 那末  $|x|^2 \geq \sum_{i=1}^k |x_i|^2$  (**Bessel-Parseval 不等式**)。再当  $V$  是有限维时,  $\{a_1, \dots, a_k\}$  是  $V$  的基底就等价于: 对于  $V$  中任意元  $x$ ,  $|x|^2 = \sum_{i=1}^k |x_i|^2$ 。

[解] 命  $\frac{a_i}{|a_i|} = e_i$ , 那末  $x_i = P_{e_i}(x) = (e_i, x) e_i$ ,  $|x_i| = e_i x$ 。

$$\begin{aligned} 0 \leq \left| x - \sum_{i=1}^k x_i \right|^2 &= \left( x - \sum_{i=1}^k x_i \right)^2 = |x|^2 - 2 \sum_{i=1}^k x_i x + \left( \sum_{i=1}^k x_i \right)^2 \\ &= |x|^2 - 2 \sum_{i=1}^k (e_i, x)^2 + \left( \sum_{i=1}^k (e_i, x) e_i \right)^2 \\ &= |x|^2 - 2 \sum_{i=1}^k (e_i, x)^2 + \sum_{i=1}^k (e_i, x)^2 = |x|^2 - \sum_{i=1}^k |x_i|^2. \end{aligned}$$

因此得 Bessel-Parseval 不等式。再

$$\text{对于任意 } x, |x|^2 = \sum_{i=1}^k |x_i|^2 \Leftrightarrow \text{对于任意 } x, x = \sum_{i=1}^k x_i,$$

即任意  $x$  能够表示为  $a_1, \dots, a_k$  的线性组合, 因此  $\{a_1, \dots, a_k\}$  成为  $V$  的基底。

**定理 22** 凡  $n$  维 Euclid 空间都相互同构<sup>①</sup>。

**证明** 由例 2,  $R^n$  形成  $n$  维 Euclid 空间。因此只要证明任意  $n$  维 Euclid 空间  $V \cong R^n$  即可。

取  $V$  的任意直交坐标系  $\varphi = \varphi(e_1, e_2, \dots, e_n)$ , 假如  $x, y \in V$ ,  $x = \sum_{i=1}^n \lambda_i e_i$ ,  $y = \sum_{i=1}^n \mu_i e_i$ , 那末

$$xy = \left( \sum_{i=1}^n \lambda_i e_i \right) \left( \sum_{i=1}^n \mu_i e_i \right) = \sum_{i=1}^n \lambda_i \mu_i = \varphi(x) \varphi(y).$$

所以  $\varphi$  是自 Euclid 空间  $V$  到  $R^n$  的同构映射。因为这样的  $\varphi$  存在, 所以  $V \cong R^n$ . (证毕)

由定理 22, 任意  $n$  维 Euclid 空间能够看成为  $R$  上  $n$  维向量空间由适当坐标系  $\varphi$  用例 2 的方法所成的 Euclid 空间。

**注意** 假定  $V$  是  $R$  上任意向量空间, 象在 §10 中所述的一样, 对于  $x \in V$ ,  $\xi \in \hat{V}$ , 定义  $(x, \xi) \in R$ , 当  $\dim V = n$  时, 如果  $\{a_1, \dots, a_n\}$  是  $V$  的基

① 假如  $R, R'$  是两个 Euclid 空间,  $\sigma$  是  $R$  到  $R'$  上的全单射, 如果

$$\sigma(x+y) = \sigma(x) + \sigma(y), \sigma(\lambda x) = \lambda \sigma(x), xy = \sigma(x) \sigma(y),$$

那末,  $\sigma$  叫做  $R$  到  $R'$  上的同构映射。这时  $R, R'$  叫做同构, 表为  $R \cong R'$ . ——译者注

底,  $\{\hat{a}_1, \dots, \hat{a}_n\}$  是它在  $\hat{V}$  中的对偶基底, 由  $\sigma: V \rightarrow \hat{V}$ ,  $\sigma(a_i) = \hat{a}_i$  ( $i=1, 2, \dots, n$ ) 就得到  $V \cong \hat{V}$ . 現在假定

$$x, y \in V, \quad x = \sum_{i=1}^n \lambda_i a_i, \quad y = \sum_{i=1}^n \mu_i a_i,$$

那末

$$(x, \sigma(y)) = \left( \sum_{i=1}^n \lambda_i a_i, \sum_{i=1}^n \mu_i \hat{a}_i \right) = \sum_{i=1}^n \lambda_i \mu_i \quad (\because (a_i, \hat{a}_j) = \delta_{ij}),$$

这就是在  $V$  給定坐标系  $\varphi(a_1, \dots, a_n)$  时, Euclid 空間  $R^n$  中的內积  $\varphi(x) \varphi(y)$ . 因此如果在  $V$  中規定  $xy = (x, \sigma(y))$ , 那末  $V$  就成为 Euclid 空間. 因为  $n$  維 Euclid 空間都同构, 所以 Euclid 空間都可以看成是象上面那样形成的.

$V$  的綫性变换  $p$  如果把任意正規直交系映为正規直交系, 那末  $p$  叫做直交变换, 表示直交变换的矩陣叫做直交矩陣.  $V$  的直交变换全体的集合記成  $\mathfrak{D}(V)$ ,  $V$  是  $n$  維时, 它略記为  $\mathfrak{D}_n$ ,  $n$  級直交矩陣全体的集合記成  $\mathfrak{P}_n$ .

**例 10**  $e_V \in \mathfrak{D}(V)$ ,  $E_n \in \mathfrak{P}_n$ .

**定理 23** 假定  $V$  是 Euclid 空間, 下面各項都是  $p \in \mathfrak{D}(V)$  为直交变换的必要充分条件.

- (i)  $p$  把  $V$  的一个正規直交基底映为正規直交基底.
- (ii) 假定  $x, y \in V$ , 那末  $p(x)p(y) = xy$ .
- (iii) 假定  $x \in V$ , 那末  $|p(x)| = |x|$ .

**証明** 假定 (0) 作为  $p \in \mathfrak{D}_n$ , 我們来証明 (0)  $\Rightarrow$  (i)  $\Rightarrow$  (ii)  $\Rightarrow$  (0), (ii)  $\Leftrightarrow$  (iii).

(0)  $\Rightarrow$  (i) 是明显的.

(i)  $\Rightarrow$  (ii) 假定  $\{e_1, e_2, \dots, e_n\}$  及  $\{p(e_1), p(e_2), \dots, p(e_n)\}$  都是  $V$  的正規直交基底. 如果  $x = \sum_{i=1}^n \xi_i e_i$ ,  $y = \sum_{i=1}^n \eta_i e_i$ , 那末

$$p(x)p(y) = \left( \sum_{i=1}^n \xi_i p(e_i) \right) \left( \sum_{i=1}^n \eta_i p(e_i) \right) = \sum_{i=1}^n \xi_i \eta_i = xy.$$

(ii)  $\Rightarrow$  (0) 是明显的.

(ii)  $\Rightarrow$  (iii) 是明显的。

(iii)  $\Rightarrow$  (ii) 假定  $x, y$  是  $V$  中任意两元, 那末  $|x+y|^2 = |x|^2 + 2xy + |y|^2$ , 所以  $xy = \frac{1}{2} (|x+y|^2 - |x|^2 - |y|^2)$ . 現在假定  $p$  是滿足 (iii) 的綫性变换, 那末

$$\begin{aligned} p(x)p(y) &= \frac{1}{2} (|p(x+y)|^2 - |p(x)|^2 - |p(y)|^2) \\ &= \frac{1}{2} (|x+y|^2 - |x|^2 - |y|^2) = xy. \end{aligned}$$

**系** 直交变换不变两元間的角度。特別保存两元的直交性。

**定理 24** 下面各項都是  $P \in \mathfrak{M}(n, R)$  为直交矩陣的必要充分条件。

- (i)  $P$  的  $n$  个列向量成为  $R^n$  的完全正規直交系。
- (ii)  $P$  的  $n$  个行向量成为  $R^n$  的完全正規直交系。
- (iii)  $P$  正則,  $P^{-1} = {}^tP$ .

**証明** 假定 (0) 作为  $P \in \mathfrak{M}_n$ .

因为  $P$  的  $n$  个列向量是  $R^n$  的自然基底关于  $P$  的象, 所以 (0)  $\Leftrightarrow$  (i) 是明显的。

其次, 当 (i) 成立时, 如果命  $P = (a_1 a_2 \cdots a_n)$ , 那末

$${}^t P P = \begin{pmatrix} {}^t a_1 \\ {}^t a_2 \\ \vdots \\ {}^t a_n \end{pmatrix} (a_1 a_2 \cdots a_n) = \begin{pmatrix} {}^t a_1 a_1 & {}^t a_1 a_2 & \cdots & {}^t a_1 a_n \\ {}^t a_2 a_1 & {}^t a_2 a_2 & \cdots & {}^t a_2 a_n \\ \cdots & \cdots & \cdots & \cdots \\ {}^t a_n a_1 & {}^t a_n a_2 & \cdots & {}^t a_n a_n \end{pmatrix}.$$

因为这里  ${}^t a_i a_j$  就是  $a_i$  与  $a_j$  的内积, 所以  ${}^t a_i a_j = \delta_{ij}$ . 于是

$${}^t P \cdot P = E_n. \quad (\text{A})$$

如果考虑 (A) 两边的行列式, 那末  $|P|^2 = 1$ , 所以  $|P| = \pm 1 \neq 0$ , 因此  $P$  正則, 于是  $P$  的逆矩陣存在。由 (A) 得  $P^{-1} = {}^t P$ . 因此 (iii) 成立。反之, 假如 (iii) 成立, 于是 (A) 成立, 因此  ${}^t a_i a_j = \delta_{ij}$  成

立, 所以 (i) 成立, 因此  $(i) \Leftrightarrow (iii)$ .

由以上的証明可得到

$$(ii) \Leftrightarrow {}^tP \in \mathfrak{P}_n \Leftrightarrow ({}^tP)^{-1} = {}^t(P^{-1}) \Leftrightarrow {}^t(P^{-1}) = P \Leftrightarrow (iii).$$

**系** 假如  $P \in \mathfrak{P}_n$ , 那末  $|P| = \pm 1$ .

**例 11** 假如  $P, P_1, P_2 \in \mathfrak{P}_n$ , 那末  ${}^tP = P^{-1} \in \mathfrak{P}_n, P_1P_2 \in \mathfrak{P}_n$ .

[解] 第一式是显然的。第二式由  $(P_1P_2)^t(P_1P_2) = P_1P_2{}^tP_2{}^tP_1 = E_n$  即得。

**例 12** 命  $\mathfrak{P}_n^+ = \{P; P \in \mathfrak{P}_n, |P| = 1\}$ ,  $\mathfrak{P}_n^- = \{P; P \in \mathfrak{P}_n, |P| = -1\}$ . 如果  $P, P_1, P_2 \in \mathfrak{P}_n^+$ , 那末  ${}^tP = P^{-1} \in \mathfrak{P}_n^+, P_1P_2 \in \mathfrak{P}_n^+$ .  $\mathfrak{P}_n^+$  中元叫做特征直交矩阵,  $\mathfrak{P}_n^-$  中元叫做非特征直交矩阵。

## § 17 实数体与复数体, 酉空間

我們在 § 3 ~ § 13 中, 假定基础体  $K$  是任意体; 在 § 14 ~ § 15, 假定  $K$  含所考虑的綫性变换的特征值, 在 § 16, 假定  $K = \mathbf{R}$ . 实数体是在体之外还具有各种性质的体。在这里不叙述以它的性质为特征的公理 (参照微积分学的教科书, 例如彌永·龟谷·田村: 微分积分学 15 ~ 19 頁)。在前节常常引用的  $\mathbf{R}$  的性质有

(i) 假如  $x_i \in \mathbf{R}, i = 1, \dots, k$ , 那末  $\sum_{i=1}^k x_i^2 \geq 0$ ,

(ii) 假如  $\sum_{i=1}^k x_i^2 = 0, x_i \in \mathbf{R}$ , 那末  $x_1 = \dots = x_k = 0$ .

因为 (i) 对于  $k=1$  也成立, 所以  $x^2 \geq 0$ . 于是負数在  $\mathbf{R}$  中沒有平方根。反之,

(iii) 假如  $a \in \mathbf{R}, a \geq 0$ , 那末  $x^2 = a$  在  $\mathbf{R}$  中有两个根  $\pm \sqrt{a}$ . 这也是  $\mathbf{R}$  的重要性质。

当  $a < 0$  时, 为了使  $x^2 = a$  能解, 于  $\mathbf{R}$  “添加”  $\sqrt{-1}$  而做成复数体  $\mathbf{C}$ . 在 § 7, 例 13 中也曾提及  $\mathbf{C}$  是  $\mathbf{R}$  上二次代数。它的元  $\xi$  能够唯一地写成  $\alpha + \beta\sqrt{-1} (\alpha, \beta \in \mathbf{R})$  的形状,  $\mathbf{C}$  中元

$$\xi = \alpha + \beta\sqrt{-1}, \bar{\xi} = \alpha - \beta\sqrt{-1} \quad (1)$$

叫做互为共轭复数。对于  $\xi$ , 使  $\bar{\xi}$  与之对应的  $\mathbf{C}$  到它自身的变换, 用  $\sigma$  表示:  $\sigma(\xi) = \bar{\xi}$ . 显然,  $\sigma\sigma = e_c$  (恒等映射)。因此  $\sigma$  是全单射, 并且  $\sigma^{-1} = \sigma$ . 又  $\sigma(\xi + \eta) = \sigma(\xi) + \sigma(\eta)$ ,  $\sigma(\xi\eta) = \sigma(\xi)\sigma(\eta)$ . 所以  $\sigma$  是将  $\mathbf{C}$  映成自身作为体的同构映射 (这事实叫做  $\sigma$  是  $\mathbf{C}$  的自同构映射)。但

$$\sigma(\xi) = \xi \Leftrightarrow \xi \in R,$$

因此  $R$  与对于  $\sigma$  “不动元”的集合一致。

$$\text{再由 (1), } \xi + \sigma(\xi) = \xi + \bar{\xi} = 2\alpha,$$

$$\xi \cdot \sigma(\xi) = \xi\bar{\xi} = \alpha^2 + \beta^2$$

都是  $R$  中元, 它們分別叫做  $\xi$  的迹 (Spur) 及范数 (Norm). 由  $R$  的性质 (i),  $\xi\bar{\xi} \geq 0$ , 非負实数  $\sqrt{\xi\bar{\xi}}$  叫做  $\xi$  的绝对值, 用  $|\xi|$  表示。

由  $R$  的性质 (ii),

$$\xi = 0 \Leftrightarrow |\xi| = 0.$$

当  $|\xi| \neq 0$ ,  $\xi = \alpha + \beta\sqrt{-1}$  时, 象

$$\cos \theta = \frac{\alpha}{|\xi|}, \quad \sin \theta = \frac{\beta}{|\xi|}$$

这样的角  $\theta$  存在, 并且能够写成

$$\xi = |\xi| (\cos \theta + i \sin \theta).$$

它叫做  $\xi$  的极式表示, 这些事实想都是周知的。

$\mathbf{C}$  的再一个重要性质 (在 § 14 中也曾说过) 是“以  $\mathbf{C}$  作系数的任意代数方程的根都在  $\mathbf{C}$  中”。这事实表达为“ $\mathbf{C}$  是代数的闭体”。

由于这最后的性质, 所以在代数上  $\mathbf{C}$  比  $R$  容易处理, 通常, 为了証明关于  $R$  的命题, 总是先把  $R$  扩张到  $\mathbf{C}$ , 然后把所得结果“缩小”到  $R$  而达到目的。把 Euclid 空間扩张成为下面定义的西空間就是这个目的。

$\mathbf{C}$  上向量空間  $U$ , 假如滿足下面条件  $U1 \sim U5$ , 那末  $U$  叫做酉 (unitary) 的, 酉的  $\mathbf{C}$  上向量空間叫做一般酉空間。特別, 有限

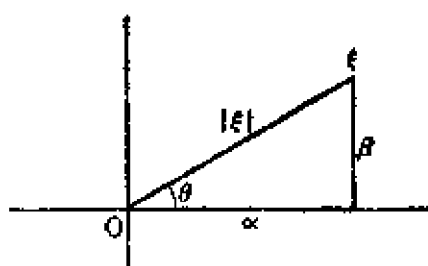


图 17.1

維的一般酉空間叫做酉空間。

**U 1.** 对于  $x, y \in U$ , 有叫做  $x, y$  的内积而用  $(x, y)$  表示的  $C$  中元与它对应。

$$U 2. (x, y) = \overline{(y, x)}.$$

$$U 3. (x_1 + x_2, y) = (x_1, y) + (x_2, y).$$

$$U 4. \text{ 对于任意 } \xi \in C, \text{ 有 } (\xi x, y) = \xi(x, y).$$

$$U 5. \text{ 由 } U 2, (x, x) \in R, \text{ 但 } (x, x) \geq 0, (x, x) = 0 \Leftrightarrow x = 0.$$

**例 1** 固定  $y$ , 命  $f(x) = (x, y)$ , 那末  $f \in \mathfrak{L}(U, C)$ , 特别  $(0, y) = 0$ . 又固定  $x$ , 命  $g(y) = (x, y)$ , 那末  $g$  在下面的意义下成为自  $U$  到  $C$  的“反綫性映射”。

一般, 假如  $U_1, U_2$  是  $C$  上向量空間,  $f: U_1 \rightarrow U_2$ , 如果条件: (a)  $x, y \in U_1$  时,  $f(x+y) = f(x) + f(y)$ , (b)  $\xi \in C$  时,  $f(\xi x) = \bar{\xi} f(x)$  成立, 那末  $f$  叫做自  $U_1$  到  $U_2$  的**反綫性映射** (anti-linear mapping)。这时,

$$f\left(\sum_{i=1}^k \xi_i x_i\right) = \sum_{i=1}^k \bar{\xi}_i f(x_i).$$

自  $U_1$  到  $U_2$  的反綫性映射全体的集合用  $\bar{\mathfrak{L}}(U_1, U_2)$  表示。  $\bar{\mathfrak{L}}(U, U)$  写成  $\bar{\mathfrak{L}}(U)$ 。对于上面的  $g, g \in \bar{\mathfrak{L}}(U, C)$ , 特别  $x \cdot 0 = 0$ 。

**例 2**  $U$  是  $C$  上  $n$  維向量空間时, 固定  $U$  的坐标系  $\varphi$ , 对于

$$\varphi(x) = \begin{pmatrix} \xi_1 \\ \vdots \\ \xi_n \end{pmatrix}, \quad \varphi(y) = \begin{pmatrix} \eta_1 \\ \vdots \\ \eta_n \end{pmatrix},$$

命  $(x, y) = {}^t\varphi(x) \cdot \overline{\varphi(y)} = \sum_{i=1}^n \xi_i \bar{\eta}_i$ , 那末  $U$  成为酉的。

特别  $C^n$  由  $(x, y) = {}^t x \cdot \bar{y}$  成为酉的。

**例 3** 当  $\alpha, \beta \in R, [\alpha, \beta] = \Delta$  时, 对于  $\mathfrak{E}(\Delta, C)$  中元  $f, g, \dots$ , 如果規定  $(f, g) = \int_{\alpha}^{\beta} f(x) \overline{g(x)} dx$ , 那末  $\mathfrak{E}(\Delta, C)$  成为酉的。

**例 4**  $|x| = \sqrt{(x, x)} \in R$ , 叫做  $x$  的长。

$$|\xi x| = |\xi| \cdot |x|, \quad |x| = 0 \Leftrightarrow x = 0.$$

对于一般酉空間及酉空間能够与一般 Euclid 空間及 Euclid 空間平行地进行討論。証明与前节完全一样, 所以把它省略。只把主要結果列举于下。以下如不預先声明, 总假定  $U$  是一般酉



空間,  $x, y, \dots$  是其中元。

**命題 45'**  $(x, y)^2 \leq |x|^2 \cdot |y|^2$ .

**命題 46'**  $|x+y| \leq |x| + |y|$ .

当  $(x, y) = 0$  时,  $x, y$  叫做**垂直或直交**, 写成  $x \perp y$ . 关于  $U$  的子空間的直交与一般 Euclid 空間同样定义, 也能得到同样結果。特別, 正規直交系、正規直交基底、完全正規直交系都与一般 Euclid 空間、Euclid 空間同样定义。

**定理 20'** 定理 20 中的 Euclid 空間  $V$  代以西空間  $U$  时也成立。

**系** 西空間具有正規直交基底。

**定理 21'** 假定  $W$  是一般西空間  $U$  的有限維子空間, 那末

$$U = W \oplus W^\perp.$$

正射影  $P_W, P_{W^\perp}$  的定义也与一般 Euclid 空間一样。

**例 5** 在一般西空間, Bessel-Parseval 不等式也成立。

**定理 22'**  $n$  維西空間都是同构。

假如  $U$  的綫性变换  $q$  把任意正規直交系映为正規直交系, 那末  $q$  叫做**酉变换**, 表示酉变换的矩陣叫做**酉矩陣**。  $U$  的酉变换全体的集合記成  $\mathfrak{U}(U)$ , 当  $U$  是  $n$  維时, 它略記为  $\mathfrak{U}_n$ .  $n$  級酉矩陣全体的集合, 記为  $\mathfrak{D}_n$ .

**定理 23'** 当  $U$  是酉空間时, 下面各項都是  $q \in \mathfrak{U}(U)$  为酉变换的必要充分条件。

(i)  $q$  把  $U$  的一个正規直交基底映为正規直交基底。

(ii) 假如  $x, y \in U$ , 那末  $(q(x), q(y)) = (x, y)$ .

(iii) 假如  $x \in U$ , 那末  $|q(x)| = |x|$ .

**系** 酉变换保存两元的直交性。

**定理 24'** 下面各項都是  $Q \in \mathfrak{M}(n, C)$  为酉矩陣的必要充分条件:

- (i)  $Q$  的  $n$  个列向量形成  $C^n$  的完全正規直交系。
- (ii)  $Q$  的  $n$  个行向量形成  $C^n$  的完全正規直交系。
- (iii)  $Q$  是正則,  $Q^{-1} = \bar{Q}$ .

系 假如  $Q \in \mathcal{D}_n$ , 那末  $Q$  的絕對值等于 1.

## § 18 正 規 變 換

在 § 13~§ 15 中我們曾考虑过下面这样的問題。

**問題 A** 当  $V$  是有限維向量空間,  $f$  是  $V$  的綫性变换时, 适当选择  $V$  中坐标系  $\varphi$ , 使得对于  $\varphi$ , 表示  $f$  的矩陣  $F$  的形状尽可能簡單。

这問題在 § 14 中引入的条件——基础体含  $f$  的特征值——下在 § 15 中已經解决了, 当  $V$  是 Euclid 空間或酉空間时, 可以考虑特別取  $\varphi$  为正規直交坐标系来解答这問題。一般的解决是困难的, 但当  $V$  是酉空間时, 由适当的正規直交坐标表为对角綫型的变换則比較容易(后面的定理 25)。并且由它能够引出关于 Euclid 空間中变换的有用結論(定理 26, 27)。

我們的目的是在关于 Euclid 空間的定理 26, 27, 酉空間与它的变换是作为手段而被引用的。因此, 我們先从 Euclid 空間經“系数擴張”作出酉空間入手。

假定  $V$  是  $n$  維 Euclid 空間, 固定它的一个正規直交基底  $\{e_1, \dots, e_n\}$ ,  $\varphi_0$  是相应于这基底的坐标系, 因为

$$V = \left\{ \sum_{i=1}^n \alpha_i e_i; \alpha_i \in \mathbf{R} \right\},$$

如果命  $U = \left\{ \sum_{i=1}^n \xi_i e_i; \xi_i \in \mathbf{C} \right\}$ , 那末  $U \supset V$ , 这时  $U$  可以看成  $\mathbf{C}$  上  $n$  維向量空間。假如在  $U$  中  $\{e_1, \dots, e_n\}$  成为正規直交基底(参照前节例 2), 那末  $U$  是  $n$  維酉空間。这时,  $U$  叫做由  $V$  經系数扩大而成的酉空間, 写成  $U = \tilde{V}$ . 又这时  $V$  中元叫做  $U$  的实向量。对

于  $x = \sum_{i=1}^n \xi_i e_i \in U$ , 叫  $\sum_{i=1}^n \bar{\xi}_i e_i \in U$  做  $x$  的共轭向量, 用  $\bar{x}$  表示。假如对于  $x$ , 使  $\bar{x}$  与之对应的映射是  $\sigma$ , 那末  $\sigma\sigma = e_U$ . 因此  $\sigma$  是全单射, 是  $U$  到自身上的反线性映射。  $U$  中对于  $\sigma$  不动的元, 即  $x = \sigma(x) = \bar{x}$  的  $x$ , 就是实向量。

以上, 由  $n$  维 Euclid 空间  $V$  的坐标系  $\varphi_0$ , 定义了  $\tilde{V}$  同  $\sigma$ . 但由  $V$  的另外任意坐标系 (可以不一定是正规直交)  $\psi$ , 也能够作出完全同样的定义。为了区别它们, 把由  $\psi$  定义的写成  $\tilde{V}_\psi, \sigma_\psi$ .

**命题 49**  $\tilde{V}_\psi = \tilde{V}, \sigma_\psi = \sigma$ .

**证明** 假定  $\{e'_1, \dots, e'_n\}$  是  $V$  给出坐标系  $\psi$  的基底, 如果

$$e'_i = \sum_{k=1}^n \lambda_{ki} e_k \quad (\lambda_{ki} \in \mathbf{R}),$$

那末

$$\tilde{V}_\psi \ni x = \sum_{i=1}^n \xi_i e'_i = \sum_{i=1}^n \xi_i \left( \sum_{k=1}^n \lambda_{ki} e_k \right) = \sum_{k=1}^n \left( \sum_{i=1}^n \xi_i \lambda_{ki} \right) e_k.$$

因为  $\xi_i \in \mathbf{C}, \lambda_{ki} \in \mathbf{R}$ , 所以  $\sum_{i=1}^n \xi_i \lambda_{ki} \in \mathbf{C}$ , 于是  $x \in \tilde{V}$ . 因此  $\tilde{V}_\psi \subset \tilde{V}$ .

同样  $\tilde{V} \subset \tilde{V}_\psi$ , 所以  $\tilde{V}_\psi = \tilde{V}$ .

又对于上面的  $x$ ,

$$\sigma_\psi(x) = \sum_{i=1}^n \bar{\xi}_i e'_i = \sum_{k=1}^n \left( \sum_{i=1}^n \bar{\xi}_i \lambda_{ki} \right) e_k = \sum_{k=1}^n \left( \overline{\sum_{i=1}^n \xi_i \lambda_{ki}} \right) e_k = \sigma(x).$$

因为, 这对于任意  $x \in V$  都成立, 所以  $\sigma_\psi = \sigma$ . (证毕)

由这命题, 得知没有必要在  $\tilde{V}_\psi, \sigma_\psi$  中明示这样的  $\psi$ , 因而可以简单记为  $\tilde{V}, \sigma$ .

以下, 在本节, 固定  $V$ , 因而固定  $\tilde{V} = U$  来讨论。

**命题 50** 假定  $U$  的子空间  $W$  对于  $\sigma$  不动, 即假定  $\sigma(W) = W$ , 那就有  $V$  的某子空间  $W_0$  存在, 使得  $W = \tilde{W}_0$ . 又它的逆也成立。

象这样的  $U$  的子空间, 叫做实子空间。

**証明** 假定  $\{a_1, \dots, a_k\}$  是  $W$  的基底, 容易得知

$$\begin{aligned} W &= [a_1, \dots, a_k] = [\bar{a}_1, \dots, \bar{a}_k] \\ &= \left[ a_1 + \bar{a}_1, \dots, a_k + \bar{a}_k, \frac{a_1 - \bar{a}_1}{\sqrt{-1}}, \dots, \frac{a_k - \bar{a}_k}{\sqrt{-1}} \right]. \end{aligned}$$

右边的  $2k$  个向量显然都是实向量。命它們为  $c_1, \dots, c_{2k}$ , 那末, 取

$$W_0 = \left\{ \sum_{j=1}^{2k} \lambda_j c_j; \lambda_j \in R \right\}$$

即可。这是因为, 假如  $\{e'_1, \dots, e'_k\}$  是  $W_0$  的正規直交基底, 那末

$$c_j = \sum_{i=1}^k \mu_{ij} e'_i, \mu_{ij} \in R. \text{ 所以}$$

$$W \ni x = \sum_{j=1}^{2k} \xi_j c_j = \sum_{i=1}^k \left( \sum_{j=1}^{2k} \mu_{ij} \xi_j \right) e'_i.$$

反之, 假定  $W_0$  是  $V$  的子空間, 那末显然  $\bar{W}_0$  对于  $\sigma$  不动。(証毕)

对于  $U$  的綫性变换  $f \in \mathfrak{L}(U)$ ,  $f = \sigma f \sigma$  叫做  $f$  的共軛变换。显然,  $\bar{f} \in \mathfrak{L}(U)$  并且  $\bar{\bar{f}} = f$ . 特別, 当  $f = \bar{f}$  时,  $f$  叫做实变换。

**命題 51** 假定  $f$  是关于  $\varphi_0$  用矩陣  $F = (\xi_{ij}) \in \mathfrak{M}(n, C)$  表示, 那末  $\bar{f}$  是关于  $\varphi_0$  用矩陣  $\bar{F} = (\bar{\xi}_{ij}) \in \mathfrak{M}(n, C)$  表示。

**証明**  $f(e_j) = \sum \xi_{ij} e_i$ , 所以  $\bar{f}(e_j) = \sigma(\sum \xi_{ij} e_i) = \sum \bar{\xi}_{ij} e_i$ . (証毕)

矩陣  $\bar{F} = (\bar{\xi}_{ij})$  叫做  $F = (\xi_{ij})$  的共軛矩陣。特別,  $F = \bar{F}$  时,  $F$  叫做实矩陣。显然, 表示实变换的矩陣是实矩陣。实矩陣是  $\mathfrak{M}(n, R)$  中元。

$f \in \mathfrak{L}(U)$  用实矩陣  $F$  表示时, 表示  $f|V$  的矩陣显然是同样。特別,  $f$  是实变换与  $f|V \in \mathfrak{L}(V)$  等价。

**命題 52** 实变换把任意实子空間映为实子空間。

**証明** 假定  $f$  是实变换,  $W$  是  $U$  的实子空間。对于  $f(W)$  中任意元  $y$ , 如果  $y = f(x)$ ,  $x \in W$ . 因为  $f = \bar{f}$ ,  $\bar{x} \in W$ , 那末  $\bar{y} = \sigma f(x) = \sigma f \sigma(\bar{x}) = \bar{f}(\bar{x}) = f(\bar{x}) \in f(W)$ . 所以  $f(W)$  是实子空間。

**命題 53** 假定  $f$  是实变换, 那末  $\text{Ker } f$ ,  $\text{Im } f$  都是实子空間。

**証明** 假定  $x \in \text{Ker } f$ , 那末  $f(\bar{x}) = \sigma \bar{f}(x) = \sigma f(x) = \bar{0} = 0$ . 所以  $\bar{x} \in \text{Ker } f$ , 因此  $\text{Ker } f$  是实子空間。

又因为  $U$  自身显然是  $U$  的实子空間, 由命題 52,  $\text{Im } f = f(U)$  是  $U$  的实子空間。 (証毕)

象在 § 10 一样, 对于  $f \in \mathfrak{L}(U)$ ,  $F \in \mathfrak{M}(n, \mathbf{C})$ , 命  ${}^t f, {}^t F$  分别表示  $f, F$  的轉置变换及轉置矩陣,  ${}^t \bar{f} = {}^t(\bar{f})$  用  $f^*$  表示,  ${}^t \bar{F} = {}^t(\bar{F})$  用  $F^*$  表示, 分别叫做  $f, F$  的伴随变换及伴随矩陣。假如  $f$  关于  $\varphi_0$  (今后“关于  $\varphi_0$ ”这語有时省略) 用矩陣  $F$  表示, 那末表示  $f^*$  的矩陣显然是  $F^*$ 。

**例 1**  $(f^*)^* = f, (f+g)^* = f^* + g^*$ ;

假如  $\xi \in \mathbf{C}$ , 那末  $(\xi f)^* = \bar{\xi} f^*, (f \circ g)^* = g^* \circ f^*$ .

$f$  是实变换与  $f^* = {}^t f$  等价。

[解] 假如就表示  $f, g$  的矩陣来考虑, 那末它們都是显然的。

**命題 54** 对于  $x, y \in U$ ,  $(f(x), y) = (x, f^*(y))$ .

**証明** 假定  $F$  是表示  $f$  的矩陣, 那末  $(f(x), y) = (F \cdot \varphi_0(x), \varphi_0(y))$  ①,  $(x, f^*(y)) = (\varphi_0(x), F^* \cdot \varphi_0(y))$ . 因此, 只要証明  $(F \cdot \varphi_0(x), \varphi_0(y)) = (\varphi_0(x), F^* \cdot \varphi_0(y))$  即可。但

$$\begin{aligned} (F \cdot \varphi_0(x), \varphi_0(y)) &= {}^t(F \cdot \varphi_0(x)) \cdot \overline{\varphi_0(y)} = {}^t \varphi_0(x) \cdot {}^t F \cdot \overline{\varphi_0(y)} \\ &= {}^t \varphi_0(x) \cdot \overline{({}^t \bar{F} \cdot \varphi_0(y))} = {}^t \varphi_0(x) \cdot \overline{(F^* \cdot \varphi_0(y))} \\ &= (\varphi_0(x), F^* \cdot \varphi_0(y)). \end{aligned} \quad (\text{証毕})$$

**定理 25** 对于  $n$  維酉空間  $U$  的变换  $f$ , 下面两个条件 (i), (ii) 是等价的。

(i)  $f$  与它的伴随变换  $f^*$  可換:  $f \circ f^* = f^* \circ f$ .

(ii) 假如取  $U$  的适当正规直交坐标  $\varphi$ , 那末  $f$  关于  $\varphi$  能够用对綫型矩陣  $D$  表示。

① 因为  $\varphi_0$  是自  $U$  到  $\mathbf{C}^n$  的同构映射,  $x \rightarrow \varphi_0(x)$ , 所以  $f(x) \rightarrow F \varphi_0(x)$ , 因此  $(f(x), y) = (F \varphi_0(x), \varphi_0(y))$ . ——譯者注

**証明** (ii)  $\Rightarrow$  (i) 假定关于  $\varphi_0$ , 表示  $f$  的矩陣是  $F$ , 自  $\varphi_0$  到  $\varphi$  的坐标变换的矩陣是  $P$ , 那末由 (ii),  $PF P^{-1} = D, F = P^{-1}DP$ . 因为  $\varphi$  是正規直交坐标, 所以  $P$  是酉矩陣, 因此  $P^{-1} = {}^t\bar{P} = P^*$ . 于是  $F^* = (P^*DP)^* = P^*D^*(P^*)^* = P^*D^*P$ ,  $FF^* = P^*DP \cdot P^*D^*P = P^*DD^*P$ ,  $F^*F = P^*D^*DP$ . 但是  $D, D^* = \bar{D}$  是对角綫型的, 所以  $DD^* = D^*D$ , 因此  $FF^* = F^*F, f \circ f^* = f^* \circ f$ .

(i)  $\Rightarrow$  (ii) 为了証明这一点, 把滿足 (i) 的  $\mathfrak{N}(U)$  中元的集合写成  $\mathfrak{N}(U)$ , 或簡記为  $\mathfrak{N}$ . 首先証明下面关于  $\mathfrak{N}$  的引理 3~5.

**引理 3** 設  $f \in \mathfrak{N}, \xi \in C$ , 則  $f - \xi \in \mathfrak{N}$ .

**証明**  $(f - \xi)(f - \xi)^* = (f - \xi)(f^* - \bar{\xi}) = ff^* - \bar{\xi}f - \xi f^* + \xi\bar{\xi}$   
 $= f^*f - \bar{\xi}f - \xi f^* + \xi\bar{\xi} = (f^* - \bar{\xi})(f - \xi)$   
 $= (f - \xi)^*(f - \xi).$

**引理 4** 設  $f \in \mathfrak{N}$ , 則  $\text{Ker } f = \text{Ker } f^*$ .

**証明** 設  $f \in \mathfrak{N}$ , 則  $(f(x), f(y)) = (f^*(x), f^*(y))$  ①. 特別,  $(f(x), f(x)) = (f^*(x), f^*(x))$ . 于是  $|f(x)| = |f^*(x)|$ . 因此  $f(x) = 0 \Leftrightarrow f^*(x) = 0$ . 所以  $\text{Ker } f = \text{Ker } f^*$ .

**引理 5** 設  $f \in \mathfrak{N}, f(x) = \xi x$ , 則  $f^*(x) = \bar{\xi}x$ .

**証明** 由引理 3,  $f - \xi \in \mathfrak{N}$ . 因此, 假如  $(f - \xi)(x) = 0$ , 那末由引理 4,  $(f - \xi)^*(x) = 0$ . 即  $f^*(x) - \bar{\xi}x = 0$ .

(i)  $\Rightarrow$  (ii) 的証明 假定  $f \in \mathfrak{N}$ ,  $f$  的特征多項式是  $\Phi_f(X) = (X - \xi_1)^{r_1} \cdots (X - \xi_k)^{r_k}$  (因为基础体  $C$  是代数閉体, 所以特征值  $\xi_i \in C$ ). 为了証明 (ii), 只要証明下列两条即可:

(a) 对于各特征值  $\xi_i$  簡約次数  $\nu_i$  都是 1, 即  $\text{Ker } (f - \xi_i) = \text{Ker } (f - \xi_i)^2$  ( $i = 1, 2, \dots, k$ ).

(b) 假如  $\xi_i \neq \xi_j$ , 那末  $\text{Ker } (f - \xi_i) \perp \text{Ker } (f - \xi_j)$ .

① 因为  $(f(x), f(y)) = (x, f^*f(y)) = (x, ff^*(y)) = (f^*(x), f^*(y))$ . ——譯者注

实际上, 假如 (a), (b) 能够成立, 那末由 (a),  $\text{Ker}(f - \xi_i) = \text{Ker}(f - \xi_i)^n$ , 如果命它为  $W_i$ , 那末  $U = W_1 \oplus \cdots \oplus W_k$ , 但由 (b),  $W_i \perp W_j$  ( $i \neq j$ ), 所以, 如果自各个  $W_i$  取正规直交基底, 那末把它们合并起来就得到  $U$  的正规直交基底。

(a) 的证明。命  $f - \xi_i = g$ , 由引理 3,  $g \in \mathfrak{N}$ . 因此, 只要示明当  $g \in \mathfrak{N}$  时,  $\text{Ker } g = \text{Ker } g^2$ , 即  $g^2(x) = g(g(x)) = 0 \Rightarrow g(x) = 0$  即可。命  $g(x) = y$ , 则  $g(y) = 0$ . 由引理 4,  $g^*(y) = 0$ , 即  $g^*g(x) = 0$ . 于是

$$(g^*g(x), x) = (g(x), g(x)) = 0.$$

所以  $g(x) = 0$ . 这就证明了 (a)。

(b) 的证明。假定  $x \in \text{Ker}(f - \xi_i)$ ,  $y \in \text{Ker}(f - \xi_j)$ , 只示明  $(x, y) = 0$  即可。由  $x, y$  的定义,  $f(x) = \xi_i x$ ,  $f(y) = \xi_j y$ . 于是  $(f(x), y) = (\xi_i x, y) = \xi_i(x, y)$ . 又

$(f(x), y) = (x, f^*(y)) = (x, \xi_j y) = \xi_j(x, y)$  (由引理 5). 所以  $\xi_i(x, y) = \xi_j(x, y)$ . 但  $\xi_i \neq \xi_j$ , 所以  $(x, y) = 0$ . 这就证明了 (b)。

由以上, 定理 25 就完全证明了。 (证毕)

满足定理 25 中条件 (i) 或 (ii) 的  $U$  的变换, 叫做正规变换。表示它的矩阵叫做正规矩阵。  $F \in \mathfrak{M}(n, \mathbb{C})$  为正规矩阵的必要充分条件由 (i) 是

$$FF^* = F^*F.$$

系 假定  $f$  是正规变换,  $\xi_1, \dots, \xi_k$  是它的特征值, 如果取适当的正射影  $p_1, \dots, p_k$ , 那末

$$f = \xi_1 p_1 + \cdots + \xi_k p_k, \quad e_U = p_1 + \cdots + p_k.$$

证明 这时  $p_i$  取  $W_i = \text{Ker}(f - \xi_i)$  上的正射影即可。 (证毕)

特别,  $f = f^*$  的  $f \in \mathfrak{L}(U)$  是正规变换, 表示它的矩阵是正规矩阵。象这样的变换, 叫做 Hermite 变换, 表示它的矩阵即满足

$F = F^*$  的矩陣叫做 **Hermite 矩陣**。Hermite 變換全体的集合用  $\mathfrak{H}$  表示。

又酉變換因為滿足  $f^{-1} = f^*$ ，所以是正規變換。酉矩陣是正規矩陣。

**命題 55** Hermite 變換的特征值是實數。酉變換的特征值的絕對值是 1。

**証明** 假定  $f$  是 Hermite 變換，那末  $(f(x), y) = (x, f(y))$ 。特別， $(f(x), x) = (x, f(x))$ ，如果  $\xi \in \mathfrak{U}$ ，那就有  $f(x) = \xi x$ ， $x \neq 0$  的  $x \in U$  存在。對於這  $x$ ， $(\xi x, x) = (x, \bar{\xi} x)$ ， $\xi(x, x) = \bar{\xi}(x, x)$ ，因此  $\xi = \bar{\xi}$  即  $\xi \in R$ 。

又假如  $f$  是酉變換，那末  $(f(x), x) = (x, f^{-1}(x))$ 。如果  $\xi \in \mathfrak{U}$ ，那末  $f(x) = \xi x$ ， $x \neq 0$ 。所以  $x = f^{-1}(\xi x) = \xi f^{-1}(x)$ 。因此  $\xi^{-1}x = f^{-1}(x)$ ，於是  $(\xi x, x) = (x, \xi^{-1}x)$ ， $\xi(x, x) = \bar{\xi}^{-1}(x, x)$ 。所以  $\xi \bar{\xi} = 1$ ，即  $|\xi| = 1$ 。 (証畢)

$F = {}^tF$  的矩陣叫做**對稱矩陣**，用對稱矩陣表示的變換叫做**對稱變換**。

**命題 56** 實矩陣是 Hermite 矩陣與它是对稱矩陣等價 (因此實變換是 Hermite 變換與它是对稱變換等價)。又實矩陣是酉矩陣與它是直交矩陣等價 (因此實變換是酉變換與它是直交變換等價)。

**証明** 由定義自明。

**定理 26** 實對稱矩陣  $F$ ，假如用適當的直交矩陣  $P$  變換，那就成為下面的對角綫型矩陣

$$PFP^{-1} = \begin{pmatrix} \alpha_1 & & 0 \\ & \ddots & \\ 0 & & \alpha_n \end{pmatrix}.$$

這裡  $\alpha_i$  ( $i=1, \dots, n$ ) 是  $f$  的特征值，它們都是實數。



**証明** 因为  $F$  是 Hermite 矩陣, 由适当的酉矩陣  $P$  变换能够成为

$$PFP^{-1} = \begin{pmatrix} \alpha_1 & & 0 \\ & \ddots & \\ 0 & & \alpha_n \end{pmatrix}, \quad (18.1)$$

这由定理 25 明白。这里  $\alpha_1, \dots, \alpha_n$  是  $F$  的特征值, 所以它們都是实数, 这在命题 55 已明示。

因为  $F$  是实矩陣,  $\alpha_i$  是实数, 所以容易理解  $F - \alpha_i$  是实变换。于是  $W_i = \text{Ker}(F - \alpha_i)$  是实子空間。由命题 50,  $W_i = \widetilde{W}_{i0}$ ,  $W_{i0} \subset V$ 。

因此, 可以取  $W_{i0}$  的正规直交基底作为  $W_i$  的正规直交基底。假如把它們合并起来做成的  $U$  的正规直交基底作为  $\varphi$ , 因为它們只是由实向量构成的, 所以, 如果把自  $\varphi_0$  到  $\varphi$  上的坐标变换的矩陣作为  $P$ , 那末  $P$  是实矩陣并且滿足 (18.1)。因此  $P$  是滿足 (18.1) 的直交矩陣。

**例 2** 試用适当的直交矩陣  $P$  变换实对称矩陣  $F' = \begin{pmatrix} 1 & 3 & 0 \\ 3 & -1 & -1 \\ 0 & -1 & 1 \end{pmatrix}$  成为对角綫型。

[解]  $\varphi_{F'}(X) = X^3 - X^2 - 11X + 11 = (X-1)(X^2-11)$ , 因此特征值是 1,  $\sqrt{11}$ ,  $-\sqrt{11}$ 。于是由适当的直交矩陣  $P$  应该得到

$$PFP^{-1} = PF'P = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \sqrt{11} & 0 \\ 0 & 0 & -\sqrt{11} \end{pmatrix}. \quad (A)$$

因为

$$\text{Ker}(F - E) = \lambda \begin{pmatrix} 1 \\ 0 \\ 3 \end{pmatrix} = \lambda \begin{pmatrix} 1 \\ \sqrt{10} \\ 0 \\ 3 \\ \sqrt{10} \end{pmatrix}, \quad \text{Ker}(F \mp \sqrt{11}E) = \lambda \begin{pmatrix} 3 \\ \sqrt{22 \mp 2\sqrt{11}} \\ \pm \sqrt{11} - 1 \\ \sqrt{22 \mp 2\sqrt{11}} \\ 1 \\ -\sqrt{22 \mp 2\sqrt{11}} \end{pmatrix},$$

所以

$$P^{-1} = \begin{pmatrix} \frac{1}{\sqrt{10}} & \frac{3}{\sqrt{22-2\sqrt{11}}} & \frac{3}{\sqrt{22+2\sqrt{11}}} \\ 0 & \frac{\sqrt{11}-1}{\sqrt{22-2\sqrt{11}}} & -\frac{\sqrt{11}+1}{\sqrt{22+2\sqrt{11}}} \\ \frac{3}{\sqrt{10}} & -\frac{1}{\sqrt{22-2\sqrt{11}}} & -\frac{1}{\sqrt{22+2\sqrt{11}}} \end{pmatrix},$$

$$P = {}^t P^{-1} = \begin{pmatrix} \frac{1}{\sqrt{10}} & 0 & \frac{3}{\sqrt{10}} \\ \frac{3}{\sqrt{22-2\sqrt{11}}} & \frac{\sqrt{11}-1}{\sqrt{22-2\sqrt{11}}} & -\frac{1}{\sqrt{22-2\sqrt{11}}} \\ \frac{3}{\sqrt{22+2\sqrt{11}}} & -\frac{\sqrt{11}+1}{\sqrt{22+2\sqrt{11}}} & -\frac{1}{\sqrt{22+2\sqrt{11}}} \end{pmatrix}.$$

如果, 試用这  $P$  实际計算就能够証实(A).

**例 3** 假定  $f$  是任意 Hermite 变换, 因为  $i, -i \notin \mathbb{C}_f$ , 所以  $(f+i)^{-1}, (f-i)^{-1} \in \mathfrak{L}(U)$ . 今命

$$q = (f+i)(f-i)^{-1},$$

那末

$$q = (f-i)^{-1}(f+i)$$

$$((f-i)q = (f-i)(f+i)(f-i)^{-1} = (f^2+1)(f-i)^{-1} = (f+i)(f-i)(f-i)^{-1} = f+i),$$

因此, 把它又写成

$$q = \frac{f+i}{f-i}. \quad (1)$$

这里  $(f-i)q = f+i$ . 如果考虑两边的伴随变换, 注意  $f^* = f$ , 那末  $q^*(f+i) = f-i$ , 所以  $q^* = (f-i)(f+i)^{-1} = q^{-1}$ . 于是用(1)定义的  $q$  是酉变换. 并且, 如果  $q(x) = x$ , 那末  $(f-i)x = (f+i)x$ . 因此  $x=0$ , 所以  $1 \notin \mathbb{C}_q$ .

反之, 假如  $q \in \mathfrak{U}$ ,  $\mathbb{C}_q \not\ni 1$ , 由

$$f = i \frac{q+1}{q-1} \quad (2)$$

定义的  $f \in \mathfrak{L}(U)$ , 因为  $f^* = f$ , 所以  $f \in \mathfrak{S}$ .

因为(2)是由(1)解  $f$  得到的, 所以(1)的关系给出  $\mathfrak{S}$  与  $\mathfrak{U}' = \{q; q \in \mathfrak{U}, \mathbb{C}_q \not\ni 1\}$  之間一一的对应. 但 Hermite 矩陣能够立刻写出, 所以特征值不是 1 的酉矩陣都能够由变换(1)得到. (1), (2)叫做 **Cayley 变换**.

**命题 57** 假定  $p$  是  $n$  維 Euclid 空間的(实)直交变换, 那末它

的特征多项式  $\Phi_p(X)$  在  $C$  中能够因子分解为下面形状:

$$\Phi_p(X) = (X-1)^{\rho_0} (X+1)^{\rho_1} (X-\varepsilon(\theta_1))^{v_1} (X-\varepsilon(-\theta_1))^{v_1} \cdots \\ (X-\varepsilon(\theta_l))^{v_l} (X-\varepsilon(-\theta_l))^{v_l}, \quad (18.2)$$

这里,  $\rho_0 \geq 0$ ,  $\rho_1 \geq 0$ ,  $v_i \geq 0$ ,  $n = \rho_0 + \rho_1 + 2(v_1 + \cdots + v_l)$ ,

$$\varepsilon(\theta) = \cos \theta + \sqrt{-1} \sin \theta.$$

**証明** 因为  $p$  的特征值的绝对值是 1, 所以  $\Phi_p(X)$  的根是 1,  $-1$  或形状如  $\varepsilon(\theta)$  的复数。于是要証明命题 57, 只要証明: 假如  $\Phi_p(X)$  有非实数根  $\xi$ , 那末  $\bar{\xi}$  也是  $\Phi_p(X)$  的同重度的根即可。

因为  $p$  是实变换, 所以  $\Phi_p(X)$  的系数都是实数, 即

$$\Phi_p(X) = \sum_{i=0}^n \alpha_i X^i, \quad \alpha_i \in R.$$

今假定  $\Phi_p(\xi) = \sum_{i=0}^n \alpha_i \xi^i = 0$ , 考虑两边的共轭复数就得到  $\sum_{i=0}^n \alpha_i \bar{\xi}^i = 0$ , 所以  $\bar{\xi}$  也是  $\Phi_p(X)$  的根。因此  $\Phi_p(X)$  能够用  $(X-\xi)(X-\bar{\xi}) = X^2 - (\xi + \bar{\xi})X + \xi\bar{\xi}$  ( $\xi + \bar{\xi} \in R$ ,  $\xi\bar{\xi} \in R$ ) 除尽, 它的商  $\psi(X)$  又以  $\xi$  与  $\bar{\xi}$  同时作为根或同时不作为根, 重复这样做下去就得知  $\Phi_p(X)$  的根  $\xi, \bar{\xi}$  的重度相等。

**定理 27** 假定  $P$  是直交矩陣, 它的特征多项式能够象 (18.2) 那样因子分解, 如果用适当的直交矩陣  $Q$  变换  $P$ , 那就成为下面的形状:

$$QPQ^{-1}$$

$$= E_{\rho_0} \oplus (-E_{\rho_1}) \oplus \underbrace{P(\theta_1) \oplus \cdots \oplus P(\theta_1)}_{v_1 \uparrow} \oplus \cdots \oplus \underbrace{P(\theta_l) \oplus \cdots \oplus P(\theta_l)}_{v_l \uparrow},$$

这里  $P(\theta) = \begin{pmatrix} \cos \theta & \sin \theta \\ -\sin \theta & \cos \theta \end{pmatrix}$ ,  $\rho_0 = 0$  或  $\rho_1 = 0$  时, 就分别沒有  $E_{\rho_0}$  或  $(-E_{\rho_1})$  的項。

**証明** 由命题 57 及定理 25, 假定

$$W^{(0)} = \text{Ker}(p-1), \quad W^{(1)} = \text{Ker}(p+1),$$

$$W_i = \text{Ker}(p-\varepsilon(\theta_i)), \quad W'_i = \text{Ker}(p-\varepsilon(-\theta_i)),$$

那就能够直和分解

$$U = W^{(0)} \oplus W^{(1)} \oplus W_1 \oplus W'_1 \oplus \cdots \oplus W_l \oplus W'_l$$

为直交系。于是假定  $W_i$  的正規直交基底是  $\{b_1^{(i)}, \dots, b_{\nu_i}^{(i)}\}$ , 那末  $W'_i$  的正規直交基底能够选取  $\{\bar{b}_1^{(i)}, \dots, \bar{b}_{\nu_i}^{(i)}\}$  ①. 今任意选取  $W^{(0)} \oplus W^{(1)}$  的正規直交基底  $\{a_1, \dots, a_{\rho_0 + \rho_1}\}$ , 如果新的基底取  $\{a_1, \dots, a_{\rho_0 + \rho_1}, b_1^{(1)}, \bar{b}_1^{(1)}, \dots, b_k^{(1)}, \bar{b}_k^{(1)}, \dots, b_{\nu_l}^{(l)}, \bar{b}_{\nu_l}^{(l)}\}$  的顺序, 用  $P$  表示的直交变换是  $p$  时,

$$p(b_k^{(i)}) = \varepsilon(\theta_i) \cdot b_k^{(i)}, \quad p(\bar{b}_k^{(i)}) = \varepsilon(-\theta_i) \cdot \bar{b}_k^{(i)}.$$

以下把  $b_k^{(i)}, \bar{b}_k^{(i)}, \theta_i$  分别略記为  $b, \bar{b}, \theta$  来討論。

$$\text{命} \quad c = \frac{b + \bar{b}}{\sqrt{2}}, \quad d = \frac{b - \bar{b}}{\sqrt{-2}},$$

显然  $[b, \bar{b}] = [c, d]$ , 并且  $c, d$  是实向量。又由于  $(b, \bar{b}) = 0$ , 所以  $|c| = 1, |d| = 1, (c, d) = 0$ . 再由計算, 容易得知

$$p(c) = \cos \theta \cdot c - \sin \theta \cdot d, \quad p(d) = \sin \theta \cdot c + \cos \theta \cdot d. \quad (18.3)$$

假如, 把对于各个  $b_k^{(i)}$  的  $c, d$  写成  $c_k^{(i)}, d_k^{(i)}$ , 那末

$$\{a_1, \dots, a_{\rho_0 + \rho_1}, c_1^{(1)}, d_1^{(1)}, \dots, c_k^{(1)}, d_k^{(1)}, \dots, c_{\nu_l}^{(l)}, d_{\nu_l}^{(l)}\} \quad (18.4)$$

就是由实向量构成的  $U$  的正規直交基底, 假定到这基底的坐标变换的矩陣是  $Q$ , 由 (18.3) 得

$$QPQ^{-1}$$

$$= E_{\rho_0} \oplus (-E_{\rho_1}) \oplus \underbrace{P(\theta_1) \oplus \cdots \oplus P(\theta_1)}_{\leftarrow \nu_1 \uparrow \rightarrow} \oplus \cdots \oplus \underbrace{P(\theta_l) \oplus \cdots \oplus P(\theta_l)}_{\leftarrow \nu_l \uparrow \rightarrow}.$$

因为  $Q$  是酉的并且实的, 所以它是直交矩陣。

**例 4** 由定理 27 的变换, 三級直交矩陣能够变为下面中的一种形状 (特

① 因为  $f(b_j^{(i)}) = \varepsilon(\theta_i) b_j^{(i)}$ , 于是  $f(\bar{b}_j^{(i)}) = f\sigma(b_j^{(i)}) = \sigma f(b_j^{(i)}) = \sigma(\varepsilon(\theta_i) b_j^{(i)}) = \varepsilon(-\theta_i) \bar{b}_j^{(i)}$ , 所以  $\bar{b}_j^{(i)} \in W'_i$ . 因为  $b_1^{(i)}, \dots, b_{\nu_i}^{(i)}$  是正規直交系, 显然  $b_1^{(i)}, \dots, \bar{b}_{\nu_i}^{(i)}$  也是正規直交系。再由定理 25 的证明中所示  $\varepsilon(\theta_i)$  的簡約次数都是 1, 所以  $\text{Ker}(f - \varepsilon(-\theta_i))^{\nu_i} = \text{Ker}(f - \varepsilon(-\theta_i))$ . 由 §14 定理 16,  $\text{Ker}(f - \varepsilon(-\theta_i))^{\nu_i}$  的維数是  $\nu_i$ , 因此  $W'_i$  的維数也是  $\nu_i$ . 所以  $b_1^{(i)}, \dots, \bar{b}_{\nu_i}^{(i)}$  形成  $W'_i$  的基底。——譯者注

征直交矩陣变换为  $P^+(\theta)$  的形状, 非特征直交矩陣变换为  $P^-(\theta)$  的形状):

$$P^+(\theta) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos \theta & \sin \theta \\ 0 & -\sin \theta & \cos \theta \end{pmatrix}, \quad P^-(\theta) = \begin{pmatrix} -1 & 0 & 0 \\ 0 & \cos \theta & \sin \theta \\ 0 & -\sin \theta & \cos \theta \end{pmatrix}.$$

[解] 特征值中有虚数时, 假定它的幅角是  $\theta$  即可。特征值都是实数时, 它們是 1 或 -1。例如特征值是 1, -1, -1 时, 假定  $\theta = \pi$ , 取  $\cos \theta = -1$  即可。

**例 5**  $F^* = -F$  的矩陣  $F$  叫做**反称-Hermite 矩陣**。因为, 反称-Hermite 矩陣也是正規矩陣的一种, 所以它能够用酉矩陣变为对角綫型。它的特征值都是純虚数。

实的反称-Hermite 矩陣  $F$  滿足关系  ${}^tF = -F$  的, 叫做**交代矩陣**或**歪对称矩陣**。假定它的特征值是  $0, \dots, 0, \pm\sqrt{-1}\alpha_1, \dots, \pm\sqrt{-1}\alpha_k$ , 那末它能够

用适当的直交矩陣能够变为  $O_{ii} \oplus \begin{pmatrix} 0 & \alpha_1 \\ -\alpha_1 & 0 \end{pmatrix} \oplus \dots \oplus \begin{pmatrix} 0 & \alpha_k \\ -\alpha_k & 0 \end{pmatrix}$  的形状。

## § 19 二次形式, Hermite 形式

所謂**形式**就是齐次多項式的別名, 例如

$$X + Y + Z, \quad X^2 - XY + Y^2$$

分別是变数  $X, Y, Z$  的一次形式及  $X, Y$  的二次形式。体  $K$  上变数  $X_1, \dots, X_n$  的二次形式一般形状是

$$\sum_{i=1}^n \sum_{j=1}^n \alpha_{ij} X_i X_j, \quad \alpha_{ij} \in K \quad (19.1)$$

(上面二重和的記号  $\sum_{i=1}^n \sum_{j=1}^n$  也可簡写成  $\sum_{i,j=1}^n$ )。  $\alpha_{ij}$  与  $\alpha_{ji}$  当然沒有必要是一样, 但因为

$$\alpha_{ij} X_i X_j + \alpha_{ji} X_j X_i = (\alpha_{ij} + \alpha_{ji}) X_i X_j,$$

所以如果把  $(\alpha_{ij} + \alpha_{ji})/2$  改为  $\alpha_{ij}$ , 即令

$$\alpha_{ij} = \alpha_{ji}, \quad (19.2)$$

(19.1) 的实质意义也不变。因此总是假定 (19.2) 成立。于是  $K$  上  $n$  級方陣

$$A = (a_{ij}) \quad (19.3)$$

是对称矩阵, 即  ${}^t A = A$ . 假如“变数向量”

$$\begin{pmatrix} X_1 \\ \vdots \\ X_n \end{pmatrix} \quad (19.4)$$

简单的用  $X$  表示, 那末 (19.1) 能够用矩阵的积

$${}^t X A X \quad (19.1')$$

表示。如果把  $K$  中元代变数  $X_i$ , 那末 (19.1) 或 (19.1') 的值就是  $K$  中元, 所以 (19.1') 可以看成是表示自  $K^n$  到  $K$  的映射。

**例 1** 体  $K$  上  $n$  个变数  $X_1, \dots, X_n$  的一次形式的一般形状是

$$\sum_{i=1}^n \alpha_i X_i, \quad \alpha_i \in K.$$

假如对于这  $X_1, \dots, X_n$  把  $K$  中元代入, 那末所得到的值就是  $K$  中元, 所以它能够看成为自  $K^n$  到  $K$  的映射。因为它显然是线性映射, 所以一次形式可以看成是  $K^n$  的对偶空间中元。

在几何学, 物理学中最常用的是  $K = \mathbf{R}$  的情况。我们今后以“实二次形式”为主来考虑。这时  $A$  是实对称矩阵。

在上面, 为了讨论 Euclid 空间引用酉空间; 讨论实对称矩阵时, 以考虑复数矩阵作为手段。与这同样, 讨论实二次形式时, 来考虑它的扩张 Hermite 形式。假定  $H$  是 Hermite 矩阵, 即  $H = H^* = {}^t \bar{H}$  是  $\mathbf{C}$  上的矩阵, 代替 (19.1'), 命

$$X^* H X = {}^t \bar{X} H X = (H X, X), \quad (19.1'')$$

叫它做 **Hermite 形式**。这时, 因为“变数向量”  $X$  是把  $U$  中任意元的坐标代入的“值”, 所以  $\bar{X}$  是有意义的。

因为对于  $X$  把  $U$  中任意元的坐标代入时,

$$(\overline{H X}, \bar{X}) = (X, H X) = (H^* X, X) = (H X, X),$$

所以  $(H X, X)$  的值是实数。因此  $(H X, X)$  能够看成是自  $\mathbf{C}^n$  到  $\mathbf{R}$  的映射。

仿此, (19.1') 也能够写成

$${}^tXAX = (AX, X).$$

在下面,假定  $A$  是表示  $n$  級实对称矩陣,  $H$  表示  $n$  級 Hermite 矩陣,  $(AX, X)$  表示二次形式,  $(HX, X)$  表示 Hermite 形式, 对于二次形式,  $X$  表示  $n$  維 Euclid 空間  $V$  中元, 对于 Hermite 形式,  $X$  表示  $n$  維酉空間  $U$  中元。与前节同样, 假定  $U = \tilde{V}$ , 固定  $V$  的(因而  $U$  的)一个正規直交基底  $\{e_1, \dots, e_n\}$  (及关于它的坐标系  $\varphi_0$ )。当  $x \in V$  (或  $x \in U$ ) 时, 如果

$$\varphi_0(x) = \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix}, \alpha_i \in \mathbf{R} \quad \left( \text{或 } \varphi_0(x) = \begin{pmatrix} \xi_1 \\ \vdots \\ \xi_n \end{pmatrix}, \xi_i \in \mathbf{C} \right),$$

那末, 在(19.4)中就命

$$X_i = \alpha_i \quad (\text{或 } X_i = \xi_i).$$

假如坐标自  $\varphi_0$  变为  $\varphi$  的坐标变换的矩陣是  $P$ , 因为用新坐标表示同一  $x$  的向量  $\varphi(x)$  是  $P\varphi_0(x)$ , 所以同样的二次形式 (或 Hermite 形式) 用新坐标表示, 就成为

$$(APX, PX) = ({}^tPAPX, X)$$

$$(\text{或 } (HPX, PX) = (P^*HPX, X)).$$

${}^tPAP$  (或  $P^*HP$ ) 叫做用坐标  $\varphi$  表示所給二次形式 (或 Hermite 形式) 的矩陣。由前节定理 26, 即得

**定理 28** 由适当的正規直交变换  $\varphi$ , 任意給定的二次形式能够用对角綫型矩陣表示。关于 Hermite 形式也是同样。

系 假定关于  $\varphi_0$  的变数向量  $X$  用适当的正規直交坐标  $\varphi$  表示的变数向量是  $Y$ , 那末

$$(AX, X) = \alpha_1 Y_1^2 + \dots + \alpha_n Y_n^2, \quad (19.5)$$

这里  $\alpha_i$  是  $A$  的特征值。关于 Hermite 形式也同样成为

$$(HX, X) = \beta_1 Y_1 \bar{Y}_1 + \dots + \beta_n Y_n \bar{Y}_n, \quad (19.5')$$

$\beta_i$  是  $H$  的特征值。

坐标自  $\varphi_0$  到象上面那样的  $\varphi$  的变换叫做所给的二次形式的主轴变换, 确定  $\varphi$  的正规直交基底的方向叫做它的主轴的方向。

**例 2** 用 § 18, 例 2 中的对称矩阵  $A = \begin{pmatrix} 1 & 3 & 0 \\ 3 & -1 & -1 \\ 0 & -1 & 1 \end{pmatrix}$ , 作二次形式  $f(X) = (AX, X) = X_1^2 - X_2^2 + X_3^2 - 2X_2X_3 + 6X_2X_1$ , 确定这  $f(X)$  的主轴方向, 并求变换后的“标准形”。

[解] 根据在 § 18, 例 2 计算的结果, 主轴的正规直交基底(假定用关于  $\varphi_0$  的坐标来表示)为

$$l_1 = \begin{pmatrix} \frac{1}{\sqrt{10}} \\ 0 \\ \frac{3}{\sqrt{10}} \end{pmatrix}, \quad l_2 = \begin{pmatrix} \frac{3}{\sqrt{22-2\sqrt{11}}} \\ \frac{\sqrt{11}-1}{\sqrt{22-2\sqrt{11}}} \\ -\frac{1}{\sqrt{22-2\sqrt{11}}} \end{pmatrix}, \quad l_3 = \begin{pmatrix} \frac{3}{\sqrt{22+2\sqrt{11}}} \\ -\frac{\sqrt{11}+1}{\sqrt{22+2\sqrt{11}}} \\ -\frac{1}{\sqrt{22+2\sqrt{11}}} \end{pmatrix},$$

或只表示方向,

$$l'_1 = \begin{pmatrix} 1 \\ 0 \\ 3 \end{pmatrix}, \quad l'_2 = \begin{pmatrix} 3 \\ \sqrt{11}-1 \\ -1 \end{pmatrix}, \quad l'_3 = \begin{pmatrix} 3 \\ -\sqrt{11}-1 \\ -1 \end{pmatrix}.$$

变换后的“标准形”为

$$f(X) = Y_1^2 + \sqrt{11}Y_2^2 - \sqrt{11}Y_3^2.$$

**例 3** 在 (19.5), 假定  $\min \alpha_i = \mu$ ,  $\max \alpha_i = M$ , 那末

$$\mu(x, x) \leqslant (AX, x) \leqslant M(x, x),$$

或用  $x \in V$  的任意坐标代变数向量  $X$  (以下不预先声明时,  $X$  总在这意义下使用),

$$\mu(X, X) \leqslant (AX, X) \leqslant M(X, X).$$

[解] 因为  $\mu \leqslant \alpha_i \leqslant M$ , 所以  $\mu Y_i^2 \leqslant \alpha_i Y_i^2 \leqslant M Y_i^2$  ( $i=1, \dots, n$ ). 于是  $\mu \sum_{i=1}^n Y_i^2 \leqslant \sum_{i=1}^n \alpha_i Y_i^2 \leqslant M \sum_{i=1}^n Y_i^2$ . 因为  $\varphi_0, \varphi$  都是正规直交基底, 所以  $\sum_{i=1}^n Y_i^2 = |x|^2 = (X, X)$ . 由这及 (19.5), 即得上述关系。

于是, 由此立即得下面定理。

**定理 29** 二次形式对于  $X$  的所有值不取负值的必要充分条件



是它的矩阵的特征值为非负的。且这时, 只有  $X=0$  它才为 0 的必要充分条件是特征值都为正的。

**证明** 把  $\mu$  象例 3 中那样定义, 命  $\mu = \alpha_j$ , 假如  $\mu > 0$ , 那末对于  $x \neq 0$  的任意  $x$ ,  $(AX, X) \geq \mu(x, x) > 0$ . 假如  $\mu = 0$ , 一般  $(AX, X) \geq \mu(x, x) = 0$ . 但对于给出  $Y_j = 1, Y_i = 0 (i \neq j)$  的  $Y$  的  $x (\neq 0)$ ,  $(AX, X) = 0$ . 假如  $\mu < 0$ , 那末对于上面给定  $Y$  的  $x$ ,  $(AX, X) < 0$ .

**例 4** 对于 Hermite 形式  $(HX, X)$ , 同样事实也成立。把  $x \in U$  的任意坐标代  $X$ ,  $(HX, X) \in \mathbb{R}$  是已如前述。与例 3 同样,

$$\mu(X, X) \leq (HX, X) \leq M(X, X).$$

这里  $\mu, M$  分别是  $H$  的特征值的最小值及最大值。定理 29 也仍旧适用于 Hermite 形式。

二次形式满足定理 29 的前面条件时叫做半正定形式。满足后面条件时, 叫做恒正形式或正定形式。

**定理 30** 二次形式是正定形式的必要充分条件为它的矩阵的所有主子(行列)式是正的。

**证明** 假定在二次形式  $(AX, X)$  中,  $A$  的所有主子(行列)式都是正的。把  $A$  的  $k$  级主子式的总和写成  $S_k$ , 那末  $\Phi_A(T) = \sum_{i=0}^n (-1)^i S_n \cdot T^i$ , 但  $S_n = |A|$ ,  $S_0 = 1$ ,  $T^0 = 1$  (这时特征多项式的变数用  $T$  表示)。因为  $S_{n-i}$  都是正的。所以, 如果  $T \leq 0$ , 那末  $\Phi_A(T) > 0$ . 因此  $\Phi_A(T) = 0$  的根即  $A$  的特征值都是正的。于是由定理 29,  $(AX, X)$  是恒正形式。

反之, 假定  $(AX, X)$  是正定形式, 因为它的特征值  $\alpha_1, \dots, \alpha_n$  都是正的, 所以  $|A| = \alpha_1 \cdots \alpha_n > 0$ . 次考虑  $A$  的任意主子式

$$A' = \begin{pmatrix} \alpha_{p_1 p_1} & \alpha_{p_1 p_2} & \cdots & \alpha_{p_1 p_k} \\ \alpha_{p_2 p_1} & \alpha_{p_2 p_2} & \cdots & \alpha_{p_2 p_k} \\ \cdots & \cdots & \cdots & \cdots \\ \alpha_{p_k p_1} & \alpha_{p_k p_2} & \cdots & \alpha_{p_k p_k} \end{pmatrix}.$$

对于小于  $n$  又不等于  $\nu_1, \nu_2, \dots, \nu_k$  的自然数  $l$ ,  $X_l=0$  的这样  $X$  全体的集合形成  $V$  的  $k$  維子空間  $W$ . 这时, 命

$$\begin{pmatrix} X_{\nu_1} \\ \vdots \\ X_{\nu_k} \end{pmatrix} = X',$$

那末, 对于  $X \in W$ ,  $(AX, X) = (A'X', X')$ . 于是  $(A'X', X')$  是  $k$  个变数  $X_{\nu_1}, \dots, X_{\nu_k}$  的恒正二次形式。因此它的矩陣  $A'$  的行列式是正的, 即  $|A'| > 0$ . (証毕)

例 5 对于  $A = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 2 & 3 \\ 1 & 3 & 6 \end{pmatrix}$ ,  $(AX, X)$  是正定形式。

[解]  $|A| = \begin{vmatrix} 1 & 1 & 1 \\ 1 & 2 & 3 \\ 1 & 3 & 6 \end{vmatrix} = 1.$

二級主子式  $\begin{vmatrix} 1 & 1 \\ 1 & 2 \end{vmatrix} = 1$ ,  $\begin{vmatrix} 2 & 3 \\ 3 & 6 \end{vmatrix} = 3$ ,  $\begin{vmatrix} 1 & 1 \\ 1 & 6 \end{vmatrix} = 5$ , 一次主子式是 1, 2, 6. 因为所有的主子式是正的, 所以  $(AX, X)$  是正定形式。

实际上, 如果求  $A$  的特征值就得到  $1, 4 \pm \sqrt{15}$ , 它們都是正的。

因为  $P$  是正則矩陣, 由 §9, 例 3,  $A$  与

$${}^t P A P = \begin{pmatrix} \alpha_1 & & 0 \\ & \ddots & \\ 0 & & \alpha_n \end{pmatrix} \quad (19.6)$$

有相同的秩。(19.6) 的秩是  $\alpha_1, \dots, \alpha_n$  中不为 0 的个数。假如它是  $r$ , 更假定正的个数是  $s$ , 負的个数是  $t$ ,  $r = s + t$ ,  $n = s + t + u$ ,  $s, t, u \geq 0$ . 适当更換  $\alpha_i$  的番号 (如果有必要) 就得到

$$\alpha_1, \alpha_2, \dots, \alpha_s > 0, \quad \alpha_{s+1}, \dots, \alpha_r < 0.$$

在 (19.5) 中命



$$Z_j^{(2)} = \sum_{i=1}^n \alpha_{ij} Z_i^{(1)}, \quad \alpha_{ij} \in R.$$

那末

$$\begin{aligned} & (Z_1^{(1)})^2 + \cdots + (Z_{s^{(1)}}^{(1)})^2 - (Z_{s^{(1)}+1}^{(1)})^2 - \cdots - (Z_r^{(1)})^2 \\ &= \left( \sum_{i=1}^n \alpha_{i1} Z_i^{(1)} \right)^2 + \cdots + \left( \sum_{i=1}^n \alpha_{is^{(1)}} Z_i^{(1)} \right)^2 \\ &= \left( \sum_{i=1}^n \alpha_{is^{(1)}+1} Z_i^{(1)} \right)^2 - \cdots - \left( \sum_{i=1}^n \alpha_{ir} Z_i^{(1)} \right)^2. \end{aligned} \quad (19.9)$$

于是考虑关于  $Z_i^{(1)}$ ,  $i=1, \dots, n$  的一次齐次方程

$$Z_1^{(1)} = \cdots = Z_{s^{(1)}}^{(1)} = Z_{s^{(1)}+1}^{(1)} = \cdots = Z_n^{(1)} = 0,$$

$$\sum_{i=1}^n \alpha_{is^{(1)}+1} Z_i^{(1)} = \cdots = \sum_{i=1}^n \alpha_{ir} Z_i^{(1)} = 0.$$

因为它的个数  $s^{(1)} + (n-r) + (r-s^{(2)}) = n + s^{(1)} - s^{(2)} < n$ , 而未知数  $Z_i^{(1)}$  的个数是  $n$ , 系数都是  $R$  中元, 所以在  $R$  中有  $Z_i^{(1)}$  不都是 0 的解。如果把这解代入 (19.9), 那末左边  $< 0$ , 右边  $\geq 0$ , 因而引出矛盾。 (证毕)

由定理 31,  $(AX, X)$  用  $V$  的适当 (不一定是正规直交) 坐标象 (19.8) 那样表示时,  $s, t$  是一定的。 $(s, t)$  叫做这二次形式的符号常数。

**例 6** 假定  $A = \begin{pmatrix} 1 & 2 & -3 \\ 2 & -1 & -1 \\ -3 & -1 & 4 \end{pmatrix}$ , 求二次形式  $(AX, X)$  的符号常数, 并求

变到 (19.8) 形状的变换矩阵。

[解]  $\Phi_A(T) = T^3 - 4T^2 - 15T = T(T^2 - 4T - 15)$ .

所以特征值是  $2 \pm \sqrt{19}, 0$ , 于是由适当的直交矩阵  $P$ ,

$$PAP = \begin{pmatrix} 2 + \sqrt{19} & 0 & 0 \\ 0 & 2 - \sqrt{19} & 0 \\ 0 & 0 & 0 \end{pmatrix},$$

更把它用

$$Q = \begin{pmatrix} \frac{1}{\sqrt{2+\sqrt{19}}} & 0 & 0 \\ 0 & \frac{1}{\sqrt{\sqrt{19}-2}} & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

变换就得到(19.8)的形状

$$(AX, X) = Z_1^2 - Z_2^2, \quad (19.10)$$

符号常数是  $s=1, t=1, u=1$ .

求上面直交矩阵  $P$  的计算是非常麻烦的。但是只求变到(19.10)的正規变换,在变换过程中不通过直交变换  $P$ ,象下面那样进行比较简单。

首先,因为  $\begin{vmatrix} 1 & 2 \\ 2 & -1 \end{vmatrix} = -5 \neq 0$ ,  $|A| = 0$ , 所以  $r(A) = 2$ . 于是得到一次

方程  $A \begin{pmatrix} \xi_1 \\ \xi_2 \\ \xi_3 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$  无关的(即不是 0)一组解。使用这解,命  $P = \begin{pmatrix} E_2 & \begin{pmatrix} \xi_1 \\ \xi_2 \end{pmatrix} \\ 0 & 0 \end{pmatrix}$ , 做变

换  $X = PY$ , 那末

$$(AX, X) = (APY, PY) = ({}^tPAPY, Y),$$

而  ${}^tPAP = \begin{pmatrix} E_2 & 0 \\ \xi_1 & \xi_2 & \xi_3 \end{pmatrix} \begin{pmatrix} A_0 & a \\ a & a \end{pmatrix} \begin{pmatrix} E_2 & \begin{pmatrix} \xi_1 \\ \xi_2 \end{pmatrix} \\ 0 & \xi_3 \end{pmatrix} = \begin{pmatrix} A_0 & 0 \\ 0 & 0 \end{pmatrix}.$

現在  $\begin{pmatrix} \xi_1 \\ \xi_2 \\ \xi_3 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$ ,  $P = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$ ,  ${}^tPAP = \begin{pmatrix} 1 & 2 & 0 \\ 2 & -1 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$

因此  $(AX, X) = Y_1^2 + 4Y_1Y_2 - Y_2^2 = (Y_1 + 2Y_2)^2 - 5Y_2^2.$

假如再用变换

$$\begin{cases} Z_1 = Y_1 + 2Y_2, \\ Z_2 = \sqrt{5}Y_2, \\ Z_3 = Y_3 \end{cases} \quad \text{即 } Y = P_1Z, \quad P_1 = \begin{pmatrix} 1 & \frac{2}{\sqrt{5}} & 0 \\ 0 & \frac{1}{\sqrt{5}} & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

那末

$$(AX, X) = Z_1^2 - Z_2^2,$$

自  $X$  变到  $Z$  的变换矩阵就是

$$PP_1 = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -\frac{2}{\sqrt{5}} & 0 \\ 0 & \frac{1}{\sqrt{5}} & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & -\frac{2}{\sqrt{5}} & 1 \\ 0 & \frac{1}{\sqrt{5}} & 1 \\ 0 & 0 & 1 \end{pmatrix}.$$

实际上,  $(PP_1)A(PP_1) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 0 \end{pmatrix}$ , 讀者試驗証之。

**例 7**  $n$  个变数  $X_1, \dots, X_n$  的二次多项式, 用“变数向量  $X$ ”能够表为

$$f(X) = (AX, X) + \alpha X + \alpha$$

的形状。 $(AX, X)$  是  $X$  的二次形式 (二次的“齐次部分”),  $\alpha X$  是  $X$  的一次形式  $\alpha_1 X_1 + \dots + \alpha_n X_n$ , (这里如果用  $\varphi_0(\alpha) = (\alpha_1, \dots, \alpha_n)$  这样的向量  $\alpha$ , 它就能够用内积  $(\alpha, X)$  表示.)  $\alpha$  是“绝对项”。假定  $X$  是  $n$  维 Euclid 空间  $V$  中的变向量, 那末满足  $f(X) = 0$  (但  $A \neq 0$ ) 的坐标  $X$  的“点”的集合  $C(f)$  叫做  $V$  的二次超曲面。如果  $n=2$ ,  $C(f)$  是二次曲线。如果  $n=3$ , 它就是普通意义的二次曲面。二次超曲面能够根据  $A$  的符号常数来“分类”, 譬如在二次曲线的情况,  $1 \leq s+t \leq n=2$ , 当  $s=2, t=0$  或  $s=0, t=2$  时,  $C(f)$  是椭圆, 当  $s=t=1$  时, 是双曲线, 当  $r=1$  时一般是抛物线。

## § 20 多重线性映射, 张量积

在 § 16 ~ § 19 中我们讨论了 Euclid 空间和酉空间, 现在再来讨论任意体  $K$  上向量空间。在本节中, 因为只是就  $K$  上的有限维向量空间来讨论, 所以今后将“ $K$  上的”以及“有限维”等字都省略而不一一声明。

在 § 12 中, 联系行列式的性质考虑过象下面这样的“函数  $\mathfrak{D}$ ”。 $\mathfrak{D}(x_1, \dots, x_n)$  定义于  $x_i \in V$  ( $V$  是  $n$  维向量空间) 而取  $K$  中值。但固定  $x_i$  以外的“变数”, 考虑  $\mathfrak{D}(x_1, \dots, x_n)$  只是  $x_i$  的函数时, 这  $x_i$  的函数记为  $\mathfrak{D}^i(x_i)$ ,  $\mathfrak{D}^i(x_i)$  是  $\mathfrak{L}(V, K)$  中元。扩张之就得到下面的概念。

假定  $V_1, \dots, V_m, V$  是綫性空間, “函数”  $f(x_1, \dots, x_m)$  定义于  $x_1 \in V_1, \dots, x_m \in V_m$  而取  $V$  中的值。如果固定  $x_1, \dots, x_m$  中  $x_i$  以外的元, 考虑  $f(x_1, \dots, x_m)$  只是  $x_i$  的函数, 則  $f_i(x_1^0, \dots, x_{i-1}^0, x_i, x_{i+1}^0, \dots, x_m^0)$  簡写成  $f_i(x_i)$ . 这时假如所有的  $f_i$  (即  $x_1^0, \dots, x_{i-1}^0, x_{i+1}^0, \dots, x_m^0$  任意取, 又  $i$  作为  $1, \dots, m$  中任一个) 都是  $\mathfrak{L}(V_i, V)$  中元, 那末  $f$  叫做自  $V_1, \dots, V_m$  到  $V$  的 **多重** (詳細点說是  **$m$  重**) **綫性映射**。多重綫性映射全体的集合用  $\mathfrak{L}(V_1, \dots, V_m; V)$  表示。

**例 1** 1重綫性映射不外是单綫性映射。

代替“2重”有用“双”这个詞的, 又当  $V = K$  时, 代替“映射”有叫做“形式”的。譬如 **双 1 次形式** 是  $\mathfrak{L}(V_1, V_2; K)$  中元。

以下直至命题 60, 因为是固定  $V_1, \dots, V_m, V$  来考虑, 所以把  $\mathfrak{L}(V_1, \dots, V_m; V)$  簡写成  $\mathfrak{L}$ 。

**命题 58** 对于  $f, g \in \mathfrak{L}, \alpha \in K$ , 假定用

$$(f+g)(x_1, \dots, x_m) = f(x_1, \dots, x_m) + g(x_1, \dots, x_m),$$

$$(\alpha f)(x_1, \dots, x_m) = \alpha f(x_1, \dots, x_m)$$

定义  $f+g, \alpha f$ , 那末  $\mathfrak{L}$  成为綫性空間。

証明是显然的。以下, 假定  $\dim V_i = n_i$ ,  $\varphi_i$  是  $V_i$  的坐标,  $a_1^{(i)}, \dots, a_{n_i}^{(i)}$  是  $V_i$  中确定  $\varphi_i$  的基底,  $\dim V = n$ ,  $\varphi$  是  $V$  的坐标,  $a_1, \dots, a_n$  是  $V$  中确定  $\varphi$  的基底。

**命题 59** 当  $f \in \mathfrak{L}$  时,  $f(x_1, \dots, x_m)$  的值由  $\varphi_i(x_i)$  及  $V$  中  $n_1 \cdots n_m$  个元

$$f(a_{k_1}^{(1)}, \dots, a_{k_m}^{(m)}), \quad 1 \leq k_i \leq n_i \quad (20.1)$$

来确定。又  $x_{k_1}, \dots, x_{k_m}$  ( $1 \leq k_i \leq n_i$ ) 是  $V$  中任意  $n_1 \cdots n_m$  个元时,  $\mathfrak{L}$  中使 (20.1) 的值成为  $x_{k_1}, \dots, x_{k_m}$  这样的元  $f$  是唯一存在的。

**証明** 假定  $\varphi_i(x_i) = \begin{pmatrix} \lambda_{i1} \\ \vdots \\ \lambda_{in_i} \end{pmatrix}$ , 即  $x_i = \sum_{k_i=1}^{n_i} \lambda_{ik_i} a_{k_i}^{(i)}$ 。

由多重綫性性, 显然

$$f(x_1, \dots, x_m) = \sum \lambda_{1k_1} \cdots \lambda_{mk_m} f(a_{k_1}^{(1)}, \dots, a_{k_m}^{(m)}), \quad (20.2)$$

即  $f(x_1, \dots, x_m)$  的值由  $\varphi_i(x_i)$  及 (20.1) 的值确定。又假定 (20.1) 的值为  $x_{k_1}, \dots, x_{k_m}$ ,  $f(x_1, \dots, x_m)$  的值由 (20.2) 确定, 那末  $f$  显然是  $\mathfrak{L}$  中元。

**命题 60** 对于  $1 \leq j_i \leq n_i$  ( $i=1, \dots, m$ ), 用命题 59 的記法, 由

$$\begin{cases} x_{j_1, \dots, j_m} = a_k, \\ k_1 = j_1, \dots, k_m = j_m \text{ 不成立, } x_{k_1, \dots, k_m} = 0 \end{cases} \quad (20.3)$$

确定的  $\mathfrak{L}$  中元如果是  $f_{j_1, \dots, j_m; k}$ , 那末这  $n_1 \cdots n_m$  个元形成  $\mathfrak{L}$  的基底。

**証明** 假定  $\sum \lambda_{j_1, \dots, j_m; k} f_{j_1, \dots, j_m; k} = f$ , 那末  $f(a_{j_1}^{(1)}, \dots, a_{j_m}^{(m)}) = \lambda_{j_1, \dots, j_m; k} a_k$ , 因此, 如果  $f=0$ , 那末  $\lambda_{j_1, \dots, j_m; k} = 0$ , 所以  $f_{j_1, \dots, j_m; k}$  是无关。又假定  $f$  是  $\mathfrak{L}$  中任意元, 如果对于  $f$ , (20.1) 的值  $x_{k_1}, \dots, x_{k_m} = \sum \lambda_{k_1, \dots, k_m; k} a_k$ , 显然  $f = \sum \lambda_{k_1, \dots, k_m; k} f_{k_1, \dots, k_m; k}$ 。

**系**  $\dim \mathfrak{L} = \dim V_1 \cdot \dim V_2 \cdots \dim V_m \cdot \dim V$ 。

因为由命题 60 的基底所得到的  $\mathfrak{L}$  的坐标是由  $\varphi_1, \dots, \varphi_m, \varphi$  确定的, 所以用  $(\varphi_1, \dots, \varphi_m; \varphi)$  来表示。

**注意 1** 对于坐标  $(\varphi_1, \varphi_2, \dots, \varphi_m, \varphi)$  的定法与基底的順序有关, 可参照后面例 2 的前面一段 (第 127 頁)。

**注意 2** (20.3) 也可象下面这样写,

$$f_{j_1, \dots, j_m; k} (a_{k_1}^{(1)}, \dots, a_{k_m}^{(m)}) = \left( \prod_{i=1}^m \delta_{j_i, k_i} \right) a_k. \quad (20.3')$$

**定理 32** 对于体  $K$  上有限維向量空間  $V_1, \dots, V_m$ , 存在具有下面性质 (i), (ii) 的  $K$  上向量空間  $T$ 。

(i) 自  $V_1, \dots, V_m$  到  $T$  存在一定的多重綫性映射  $\tau$ , 而且  $T$  能够用  $\tau(x_1, \dots, x_m)$ ,  $x_i \in V_i$  生成。

(ii) 假如存在自  $V_1, \dots, V_m$  到  $K$  上任意向量空間  $V$  的多重綫性映射  $f$ , 那就唯一的存在自  $T$  到  $V$  适合下面关系的綫性映射  $F$ :

$$\begin{array}{ccc} (V_1, \dots, V_m) & \xrightarrow{\tau} & T \\ & \searrow f & \downarrow F \\ & & V \end{array}$$



$$f := F \circ \tau. \quad (A)$$

又在  $T$  以外, 假如有具有性质 (i), (ii) 的  $K$  上向量空間  $T'$ , 如果自  $V_1, \dots, V_m$  到  $T'$  由 (i) 规定的多重綫性映射是  $\tau'$ , 那就有自  $T$  到  $T'$  的同构映射  $\sigma$ , 使得

$$\begin{array}{ccc} (V_1, \dots, V_m) & \longrightarrow & T \\ & \searrow & \downarrow \sigma \\ & & T' \end{array}$$

$$\tau' = \sigma \circ \tau,$$

$$\tau = \sigma^{-1} \circ \tau'.$$

**証明** 首先証明后半段“ $T$  的唯一性”。假定  $V = T'$ , 如果引用 (ii), 那末  $\tau' = \sigma \circ \tau$  这样的  $\sigma \in \mathfrak{L}(T, T')$  存在。互換  $T', T$  来同样考虑, 那就有  $\tau = \sigma' \circ \tau'$  这样的  $\sigma' \in \mathfrak{L}(T', T)$ . 于是  $\tau = \sigma' \circ \sigma \circ \tau$ . 因为由 (i),  $T$  是由  $\tau(x_1, \dots, x_m)$  生成, 所以对于  $T$  中任意元  $t$ ,  $\sigma'(\sigma(t)) = t$ , 即  $\sigma' \circ \sigma$  成为  $T$  的恒等映射。同样因为  $\sigma \circ \sigma'$  是  $T'$  的恒等映射, 所以  $\sigma' = \sigma^{-1}$ . 因此  $\sigma$  是同构映射。

次証明“ $T$  的存在”。假定  $V_i$  的对偶空間 (§ 10) 是  $\hat{V}_i$ , 它的元一般用  $\xi_i$  表示, 在

$$\mathfrak{L}(\hat{V}_1, \dots, \hat{V}_m; K) = T \quad (20.4)$$

中,  $\tau$  可以象下面这样来定义:

$$\tau(x_1, \dots, x_m)(\xi_1, \dots, \xi_m) = (\xi_1, x_1) \cdots (\xi_m, x_m). \quad (20.5)$$

(i) 用 (20.5) 定义的  $\tau(x_1, \dots, x_m)$  实际是  $T$  中元, 并且显然  $\tau \in \mathfrak{L}(V_1, \dots, V_m; T)$ . 假定坐标  $\varphi_i$  的对偶坐标是  $\hat{\varphi}_i$ , 給出它的基底是  $\{\hat{a}_1^{(1)}, \dots, \hat{a}_n^{(1)}\}$  时, 那末給出  $T$  的坐标  $(\hat{\varphi}_1, \dots, \hat{\varphi}_m)$  的基底是由适合

$$f_{j_1, \dots, j_m}(\hat{a}_{k_1}^{(1)}, \dots, \hat{a}_{k_m}^{(m)}) = \prod_{i=1}^m \delta_{j_i, k_i} \quad (20.6)$$

的  $f_{j_1, \dots, j_m}$  所构成。这是因为, 在 (20.5) 中如果命

$$\tau(a_{j_1}^{(1)}, \dots, a_{j_m}^{(m)}) = f_{j_1, \dots, j_m},$$

就正好成为 (20.6) 那样, 所以  $T$  是由这  $n_1 \cdots n_m$  个元  $\tau(a_{j_1}^{(1)}, \dots, a_{j_m}^{(m)})$  生成的。

(ii) 假如  $f(a_{j_1}^{(1)}, \dots, a_{j_m}^{(m)}) = x_{j_1, \dots, j_m} \in V$ , 为了(A)成立必須

$$F(\tau(a_{j_1}^{(1)}, \dots, a_{j_m}^{(m)})) = x_{j_1, \dots, j_m}. \quad (20.7)$$

又象上面所示, 因为  $\tau(a_{j_1}^{(1)}, \dots, a_{j_m}^{(m)})$  是  $T$  的基底, 所以由 (20.7) 能够确定  $F \in \mathfrak{L}(T, V)$ . (証毕)

具有定理 32 中性质 (i), (ii) 的向量空間  $T$  叫做  $V_1, \dots, V_m$  的張量积, 用  $V_1 \otimes \dots \otimes V_m$  或  $\bigotimes_{i=1}^m V_i$  表示。又  $\tau(x_1, \dots, x_m)$  用  $x_1 \otimes \dots \otimes x_m$  或  $\bigotimes_{i=1}^m x_i$  表示。因为  $\tau$  是多重綫性映射, 所以

$$x_1 \otimes (x_2 + y_2) = x_1 \otimes x_2 + x_1 \otimes y_2,$$

$$x_1 \otimes \alpha x_2 = \alpha(x_1 \otimes x_2).$$

又因为  $\dim V_i = n_i$ , 所以由命題 60 系,

$$\dim(V_1 \otimes \dots \otimes V_m) = \dim V_1 \cdots \dim V_m.$$

并且象上面所示,  $a_{j_1}^{(1)} \otimes \dots \otimes a_{j_m}^{(m)}$  ( $1 \leq j_i \leq n_i$ ) 构成  $V_1 \otimes \dots \otimes V_m$  的基底。在构成这个基底的  $n_1 \cdots n_m$  个元中, 任意两个元  $a = a_{j_1}^{(1)} \otimes \dots \otimes a_{j_m}^{(m)}$  与  $a' = a_{j'_1}^{(1)} \otimes \dots \otimes a_{j'_m}^{(m)}$ , 如果  $j_1 = j'_1, \dots, j_\nu = j'_\nu, j_{\nu+1} \leq j'_{\nu+1}$ , 那末把  $a$  放在  $a'$  的前面。由这順序确定的坐标用  $(\varphi_1, \dots, \varphi_m)$  表示。

**例 2** 假定  $V_1 = [a_1, a_2], V_2 = [b_1, b_2, b_3], V_3 = [c_1, c_2]$ , 那末

$$\begin{aligned} V_1 \otimes V_2 \otimes V_3 = & [a_1 \otimes b_1 \otimes c_1, a_1 \otimes b_1 \otimes c_2, a_1 \otimes b_2 \otimes c_1, a_1 \otimes b_2 \otimes c_2, \\ & a_1 \otimes b_3 \otimes c_1, a_1 \otimes b_3 \otimes c_2, a_2 \otimes b_1 \otimes c_1, a_2 \otimes b_1 \otimes c_2, \\ & a_2 \otimes b_2 \otimes c_1, a_2 \otimes b_2 \otimes c_2, a_2 \otimes b_3 \otimes c_1, a_2 \otimes b_3 \otimes c_2], \end{aligned}$$

依这順序的基底所确定的  $V_1 \otimes V_2 \otimes V_3$  的坐标是  $(\varphi_1, \varphi_2, \varphi_3)$ 。

**例 3** 在右图中, 把  $F$  与  $f$  对应得到  $\mathfrak{L}(V_1, \dots, V_m; V)$  与  $\mathfrak{L}(V_1 \otimes \dots \otimes V_m, V)$  的同构映射。

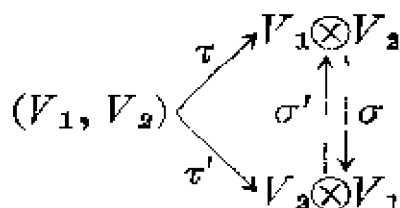
$$\begin{array}{ccc} (V_1, \dots, V_m) & \xrightarrow{\tau} & V_1 \otimes \dots \otimes V_m \\ & \searrow f & \swarrow F \\ & V & \end{array}$$

**命題 61**  $V_1 \otimes V_2$  与  $V_2 \otimes V_1$  由  $x_1 \otimes x_2 \rightarrow x_2 \otimes x_1$  对应成为同构。

**証明** 假定  $\tau(x_1, x_2) = x_1 \otimes x_2, \tau'(x_1, x_2) = x_2 \otimes x_1$ , 那末

$\tau \in \mathfrak{L}(V_1, V_2; V_1 \otimes V_2)$ ,  $\tau' \in \mathfrak{L}(V_1, V_2; V_2 \otimes V_1)$ . 再对于这, 引用

(ii) 与上面唯一性的证明同样考虑, 即得所证。



下面的命题完全同样。

**命题 62**  $(V_1 \otimes V_2) \otimes V_3 \cong V_1 \otimes (V_2 \otimes V_3) \simeq V_1 \otimes V_2 \otimes V_3$ .

**例 4**  $V \otimes K \cong V$ ,  $V_1 \otimes \hat{V}_2 \cong \mathfrak{L}(V_1, V_2)$ .

**例 5** 由  $x_1 \otimes x_2$  的多重线性性得  $x_1 \otimes 0 = 0 \otimes x_2 = 0$ . 又假如  $x_1 \otimes x_2 = 0$ , 那末  $x_1 = 0$  或  $x_2 = 0$ . (如果  $x_1 \neq 0$ ,  $x_2 \neq 0$ , 那就能够取  $x_1, x_2$  分别作为  $V_1, V_2$  的基底中元, 因此就能够把  $x_1 \otimes x_2$  作为  $V_1 \otimes V_2$  的基底中元.)

**命题 63** 假定  $f_i$  是自向量空间  $V_i$  到向量空间  $W_i$  的线性映射,  $f_i \in \mathfrak{L}(V_i, W_i)$ ,  $i = 1, \dots, m$ , 那末, 对于  $x_1 \otimes \dots \otimes x_m \in V_1 \otimes \dots \otimes V_m$ , 使  $f_1(x_1) \otimes \dots \otimes f_m(x_m) \in W_1 \otimes \dots \otimes W_m$  与之对应的  $\mathfrak{L}(V_1 \otimes \dots \otimes V_m, W_1 \otimes \dots \otimes W_m)$  中元  $f$  是唯一地存在的。

**证明**  $\mathfrak{L}(V_1 \otimes \dots \otimes V_m, W_1 \otimes \dots \otimes W_m)$  中元  $f$  如果对于  $V_1 \otimes \dots \otimes V_m$  的基底  $a_{k_1}^{(1)} \otimes \dots \otimes a_{k_m}^{(m)}$  的值  $f(a_{k_1}^{(1)} \otimes \dots \otimes a_{k_m}^{(m)})$  已给定, 它就唯一确定。现在假定

$$f(a_{k_1}^{(1)} \otimes \dots \otimes a_{k_m}^{(m)}) = f_1(a_{k_1}^{(1)}) \otimes \dots \otimes f_m(a_{k_m}^{(m)}), \quad (20.8)$$

显然  $f(x_1 \otimes \dots \otimes x_m) = f_1(x_1) \otimes \dots \otimes f_m(x_m)$ , 这就是所求的  $f$ .

(证毕)

**系** 对于  $\otimes \mathfrak{L}(V_i, W_i)$  中元  $\otimes f_i$ , 假如使上面的  $f$  与之对应, 那就得到自  $\otimes \mathfrak{L}(V_i, W_i)$  到  $\mathfrak{L}(\otimes V_i, \otimes W_i)$  上的同构映射。(系毕)

通常把  $\otimes f_i$  与  $f$  同样看待, 叫  $f$  做  $f_i$  的张量积或 Kronecker 积。

假如  $V_i, W_i$  的坐标分别是  $\varphi_i, \psi_i$ , 那末  $\otimes V_i, \otimes W_i$  分别有坐标  $(\varphi_1, \dots, \varphi_m), (\psi_1, \dots, \psi_m)$ . 假如由  $\varphi_i, \psi_i$  表示  $f_i$  的矩阵是  $F_i$ , 那末由坐标  $(\varphi_1, \dots, \varphi_m), (\psi_1, \dots, \psi_m)$  表示  $f = \otimes f_i$  的矩

陣應該如何? 假定  $F_i = (\alpha_{jk}^{(i)})$ , 因为

$$f_i(a_{k_i}^{(i)}) = \sum_{j_i=1}^{l_i} \alpha_{j_i k_i}^{(i)} b_{j_i}^{(i)} \left( l_i = \dim W_i, b_{j_i}^{(i)} \text{ 是 } W_i \text{ 中确定 } \psi_i \text{ 的基底} \right),$$

由 (20.8), 得

$$f(a_{k_1}^{(1)} \otimes \cdots \otimes a_{k_m}^{(m)}) = \sum_{j_1=1}^{l_1} \cdots \sum_{j_m=1}^{l_m} \alpha_{j_1 k_1}^{(1)} \cdots \alpha_{j_m k_m}^{(m)} b_{j_1}^{(1)} \otimes \cdots \otimes b_{j_m}^{(m)}. \quad (20.9)$$

因为确定  $V_1 \otimes \cdots \otimes V_m$  的坐标  $(\varphi_1, \cdots, \varphi_m)$  的基底正好是  $a_{k_1}^{(1)} \otimes \cdots \otimes a_{k_m}^{(m)}$ ,  $1 \leq k_i \leq n_i$ , 确定  $W_1 \otimes \cdots \otimes W_m$  的坐标  $(\psi_1, \cdots, \psi_m)$  的基底是  $b_{j_1}^{(1)} \otimes \cdots \otimes b_{j_m}^{(m)}$ ,  $1 \leq j_i \leq l_i$ , 所以由坐标  $(\varphi_1, \cdots, \varphi_m)$ ,  $(\psi_1, \cdots, \psi_m)$  表示  $f$  的矩阵显然是  $(\prod \dim W_i, \prod \dim V_i)$  型的矩阵  $F = (\alpha_{j_1 k_1}^{(1)} \cdots \alpha_{j_m k_m}^{(m)})$ . 这矩阵  $F$  不外是映射  $F_i \in \mathfrak{L}(K^{n_i}, K^{l_i})$  的张量积  $F_1 \otimes \cdots \otimes F_m$ .

**例 6** 假定  $F_1 = \begin{pmatrix} \alpha_{11} & \alpha_{12} \\ \alpha_{21} & \alpha_{22} \\ \alpha_{31} & \alpha_{32} \end{pmatrix}$ ,  $F_2 = (\beta_1, \beta_2, \beta_3)$ , 那末

$$F_1 \otimes F_2 = \begin{pmatrix} \alpha_{11}\beta_1 & \alpha_{11}\beta_2 & \alpha_{11}\beta_3 & \alpha_{12}\beta_1 & \alpha_{12}\beta_2 & \alpha_{12}\beta_3 \\ \alpha_{21}\beta_1 & \alpha_{21}\beta_2 & \alpha_{21}\beta_3 & \alpha_{22}\beta_1 & \alpha_{22}\beta_2 & \alpha_{22}\beta_3 \\ \alpha_{31}\beta_1 & \alpha_{31}\beta_2 & \alpha_{31}\beta_3 & \alpha_{32}\beta_1 & \alpha_{32}\beta_2 & \alpha_{32}\beta_3 \end{pmatrix}.$$

一般, 假定  $F_1 = (\alpha_{jk})$ , 那末

$$F_1 \otimes F_2 = \begin{pmatrix} \alpha_{11}F_2 & \alpha_{12}F_2 & \cdots & \alpha_{1n}F_2 \\ \alpha_{21}F_2 & \alpha_{22}F_2 & \cdots & \alpha_{2n}F_2 \\ \cdots & \cdots & \cdots & \cdots \\ \alpha_{n1}F_2 & \alpha_{n2}F_2 & \cdots & \alpha_{nn}F_2 \end{pmatrix}.$$

**例 7** 当  $f_1, g_1 \in \mathfrak{L}(V_1, W_1)$ ,  $\alpha \in K$  时,

$$(f_1 + g_1) \otimes f_2 \otimes \cdots \otimes f_m = f_1 \otimes f_2 \otimes \cdots \otimes f_m + g_1 \otimes f_2 \otimes \cdots \otimes f_m,$$

$$(\alpha f_1) \otimes f_2 \otimes \cdots \otimes f_m = \alpha (f_1 \otimes f_2 \otimes \cdots \otimes f_m).$$

**例 8** 假定  $f_i \in \mathfrak{L}(V_i, W_i)$ ,  $g_i \in \mathfrak{L}(W_i, U_i)$ , 那末

$$(g_1 \otimes \cdots \otimes g_m) \circ (f_1 \otimes \cdots \otimes f_m) = (g_1 \circ f_1) \otimes \cdots \otimes (g_m \circ f_m).$$

于是对于矩阵的张量积, 例 7, 8 中的式子同样成立。

假定非负的整数  $p, q$  及向量空间  $V$  已给定, 那末  $p$  个  $V$  及  $q$  个  $V'$  的张量积

$$V \otimes \cdots \otimes V \otimes \hat{V} \otimes \cdots \otimes \hat{V}$$

$$\longleftarrow p \uparrow \longrightarrow \quad \longleftarrow q \uparrow \longrightarrow$$

(这張量积的顺序即令变动, 但命题 61, 62 中产生的空間之間“标准的”同构关系仍然成立) 叫做  $V$  上的  $(p, q)$  型張量空間, 用  $T_q^p(V)$  表示.  $T_q^0(V)$  单写成  $T_q(V)$ ,  $T_0^p(V)$  单写成  $T^p(V)$ .  $T_0^0(V)$  就是  $K$ .

例 9  $T^1(V) = V$ ,  $T_1(V) = \hat{V}$ ,  $\dim T_q^p(V) = (\dim V)^{p+q}$ .

于是直和空間  $\sum_{p, q \geq 0} \otimes T_q^p(V)$  用  $T(V)$  表示, 它叫做  $V$  上張量空間, 它的元叫做  $V$  上的張量. 特別,  $T_0^0(V) = K$  中元不外是数量,  $T^1(V) = V$  中元不外是向量.  $V$  中元又叫做逆变向量. 与这对应,  $T_1(V) = \hat{V}$  中元又叫做协变向量.  $T_q^p(V)$  中元叫做逆变  $p$  阶协变  $q$  阶的張量. 当  $p > 0$ ,  $q > 0$  时也叫做混合張量.

例 10  $T(V)$  是  $K$  上无限維向量空間, 因为  $T_q^p(V)$  中元与  $T_{q'}^{p'}(V)$  中元的張量积显然成为  $T_{q+q'}^{p+p'}(V)$  中元, 所以  $T(V)$  对于这“張量乘法”成为环, 并且成为  $K$  上代数 (§ 7). 它叫做  $V$  上張量代数.

假定  $V$  的坐标  $\varphi$  确定, 那末  $\hat{V}$  对偶坐标  $\hat{\varphi}$  确定,  $T_q^p(V)$  坐标  $(\varphi, \dots, \varphi, \hat{\varphi}, \dots, \hat{\varphi})$  也确定. 这坐标如果用  $\varphi_q^p$  表示, 那末确定  $\varphi_q^p$  的  $T_q^p(V)$  的基底是  $a_{j_1} \otimes \cdots \otimes a_{j_p} \otimes \hat{a}_{k_1} \otimes \cdots \otimes \hat{a}_{k_q}$ ,  $1 \leq j_i \leq n$ ,  $1 \leq k_l \leq n$ .  $T_q^p(V)$  中任意元  $x$  能够表为

$$x = \sum \xi_{j_1 \dots j_p k_1 \dots k_q} a_{j_1} \otimes \cdots \otimes a_{j_p} \otimes \hat{a}_{k_1} \otimes \cdots \otimes \hat{a}_{k_q}$$

的形状.  $(\dim V)^{p+q}$  个  $K$  中元  $\xi_{j_1 \dots j_p k_1 \dots k_q}$  是  $x$  关于  $\varphi_q^p$  的坐标. 习惯上逆变的番号記在上肩, 因此它写成  $\xi_{k_1 \dots k_q}^{j_1 \dots j_p}$ .

假定  $V$  的坐标自  $\varphi$  变为  $\psi$ , 那末  $T_q^p(V)$  的坐标就自  $\varphi_q^p$  变为  $\psi_q^p$ .  $x$  关于  $\psi_q^p$  的坐标假如是  $\eta_{k_1 \dots k_q}^{j_1 \dots j_p}$ . 自  $\varphi$  到  $\psi$  的变换矩陣假如是  $P = (\pi_{kl})$ , 因为  $V$  自坐标  $\hat{\varphi}$  到  $\hat{\psi}$  的变换矩陣是  ${}^tP = (\pi_{lk})$ , 根据命题 63 后面記述的事实, 自  $\varphi_q^p$  到  $\psi_q^p$  的变换矩陣为  $P \otimes \cdots \otimes P \otimes {}^tP \otimes \cdots \otimes {}^tP$ . 假如依照习惯把  $\pi_{kl}$  記成  $\pi_l^k$ , 那末

$$\eta_{k_1 \dots k_q}^{i_1 \dots i_p} = \sum_{l_1=1}^n \dots \sum_{l_p=1}^n \sum_{h_1=1}^n \dots \sum_{h_q=1}^n \sigma_{l_1}^{i_1} \dots \sigma_{l_p}^{i_p} \sigma_{h_1}^{k_1} \dots \sigma_{h_q}^{k_q} \zeta_{h_1 \dots h_q}^{l_1 \dots l_p}, \quad (20.10)$$

在这样式子中, 和的記号  $\sum_{l_1=1}^n \dots \sum_{l_p=1}^n \sum_{h_1=1}^n \dots \sum_{h_q=1}^n$  有时簡称为 **Einstein 規約**。Einstein 在相对論的記述中, 頻繁地应用張量运算, 为簡化这种記法引入了这規約。(原来張量是定义为当坐标变换具有象 (20.10) 那样变换分量的“量”。)

以上只敘述了綫代数中最基础的事項, 但已超过預定的篇幅。本章不得不在这里停止。下面就它範圍內剩下的(包含在本丛书其他书籍中的內容)略进一言。

关于向量的內积在 § 16, § 17 中已敘述, 但关于外积就沒有接触到。一般, 它能够作为联系張量积的交代积的概念来敘述, 这在李群論一书中應該有所記述。至于向量和張量的几何学的物理学的应用都在几何学一书中介紹。

在 § 3, § 7 等的例中所敘述的各种函数空間都是向量空間, 但关于它的解析理論預定在引入适当的拓扑条件之后, 将在泛函分析、广义函数等书中討論。又关于矩陣的“解析函数” $\left(\exp F = E + F + \frac{F^2}{2!} + \frac{F^3}{3!} + \dots\right)$  在上面也沒有接触机会。在考虑它們时, 基础体的拓扑是重要的。譬如基础体是复数体  $C$  时, “指数級数”总是收斂而且有  $\exp F$  的意义。当  $F_1 F_2 = F_2 F_1$  时, 能容易証明  $\exp(F_1 + F_2) = \exp F_1 \cdot \exp F_2$  等, 这都作为讀者的练习。

## 第2章 群, Boole 代数, 有限体

在这短短的第2章里, 将就群, Boole 代数, 有限体这三种代数系分别作简单解说。其中群对于数学有一般的基本意义, 但 Boole 代数, 有限体却是相当特殊的代数系。三者之间没有特别密切的关系。只是因为这些代数系在新的应用数学的各个部分都须用到, 而在本丛书的其他书籍中没有机会介绍, 因此, 有关它们的基本事项只有在这里来叙述。

第1章关于綫代数的内容无论如何总能够进行系统的说明。下面第3章有限群的表现论亦能系统地进行叙述。但是这第2章, 由于上述那种情况, 全章不能建立一贯的体系。这点希望预先得到读者的了解(又本章中群的部分乃是第3章所必须的准备)。

### § 21 变换群的概念

作为代数系来定义群是容易的, 但这样做对于初次接受这概念的读者有“过分抽象”的缺点。因此还是按照历史的顺序从变换群的概念的说明开始。

群(group) 这个名词在数学史上开始使用的是 Galois. 根据这概念, Lagrange 等的“代数方程的形而上学”是被数学化了(参照 A. Weil “自形而上学到数学”, 科学 Vol. 26, No. 12)。下面用最简单的例子来说明 Lagrange 和 Galois 的思想方法。

读者想必已知道对称式, 交代式这些名词。譬如象  $x + y + z$ ,  $xy + yz + zx$  这样, 任意互换变数  $x, y, z$  而不变的多项式是  $x, y, z$  的对称式, 象  $(y - z)(z - x)(x - y)$ ,  $x^k(y - z) + y^k(z - x) + z^k(x - y)$  这样任意互换  $x, y, z$  中两个只改变符号的多项式是交代式。但是象  $x + 2y + 3z$  这样就既不是对称式也不是交代式。

为了明确概念, 来考虑复数体  $C$  上  $n$  个变数  $x_1, \dots, x_n$  的多

项式

$$f(x_1, \dots, x_n) = \sum \alpha_{k_1 \dots k_n} x_1^{k_1} \dots x_n^{k_n}, \quad \alpha_{k_1 \dots k_n} \in \mathcal{O}. \quad (21.1)$$

这里  $k_1, \dots, k_n$  取非负的整数值,  $\sum$  当然是意味有限和。表示变数的“互换”用下面引入的那种记法是非常方便的。假定  $(\nu_1, \nu_2, \dots, \nu_n)$  是  $n$  个文字  $(1, 2, \dots, n)$  的一个排列, 把变数的添数  $1, 2, \dots, n$  分别用  $\nu_1, \nu_2, \dots, \nu_n$  代换的事实用

$$\begin{pmatrix} 1 & 2 & \dots & n \\ \nu_1 & \nu_2 & \dots & \nu_n \end{pmatrix} \quad (21.2)$$

表示。象这样的互换叫做置换。置换也有用  $\pi, \kappa, \dots$  等文字来表示的。今假定(21.2)的置换是  $\pi$ , 由  $n$  个文字  $1, 2, \dots, n$  形成的“空间”(为了把集合几何学地表达, 也叫它做“空间”)是  $S$ , 那末  $\pi$  是自  $S$  到  $S$  的全单射,  $\pi: S \rightarrow S$ . 在这意义下, 用函数记号写成  $\pi(i) = \nu_i$ . 对于(21.2), 在第 1 行中  $i$  之下写它的象  $\pi(i) = \nu_i$  是重要的, 而第 1 行排列为  $1, 2, \dots, n$  的顺序不是必要的。譬如

$$\pi = \begin{pmatrix} 1 & 2 & \dots & n \\ \nu_1 & \nu_2 & \dots & \nu_n \end{pmatrix} = \begin{pmatrix} 2 & 1 & 3 & \dots & n \\ \nu_2 & \nu_1 & \nu_3 & \dots & \nu_n \end{pmatrix}. \quad (21.2')$$

当  $\nu_1=1, \nu_2=2, \dots, \nu_n=n$  时, (21.2) 显然成为  $S$  的恒等映射  $\varepsilon$ . 又假如结合(21.2)的  $\pi$  与

$$\kappa = \begin{pmatrix} \nu_1 & \nu_2 & \dots & \nu_n \\ \mu_1 & \mu_2 & \dots & \mu_n \end{pmatrix}, \quad \left( \begin{matrix} \mu_1, \dots, \mu_n \text{ 是 } 1, \dots, n \\ \text{的另一个排列} \end{matrix} \right), \quad (21.3)$$

那就得

$$\kappa \circ \pi = \begin{pmatrix} 1 & 2 & \dots & n \\ \mu_1 & \mu_2 & \dots & \mu_n \end{pmatrix}.$$

特别,

$$\begin{pmatrix} \nu_1 & \nu_2 & \dots & \nu_n \\ 1 & 2 & \dots & n \end{pmatrix}$$

是  $\pi$  的逆映射  $\pi^{-1}$ . 因为  $n$  个文字有  $n!$  种排列, 所以  $S = \{1,$



$2, \dots, n\}$  的置换全体的集合  $\mathfrak{S}(S)$  是由  $n!$  个元  $\varepsilon, \pi, \kappa, \dots$  构成的。

**注意** 上面的  $\kappa \circ \pi$  也有写成  $\pi \kappa$  的。在本书是写成  $\kappa \circ \pi$ , 即把先行使的置换后写。 $\kappa \circ \pi$  与  $\pi \circ \kappa$  一般不同。

**例1** 只互换两文字 1, 2 的

$$\begin{pmatrix} 1 & 2 & 3 & \dots & n \\ 2 & 1 & 3 & \dots & n \end{pmatrix} \quad (21.4)$$

叫做 1, 2 的**互换**, 用  $(1\ 2)$  表示。又一般对于  $\pi$ , 命  $\pi^0 = \varepsilon, \pi^1 = \pi, \pi^2 = \pi\pi, \dots, \pi^k = (\pi^{k-1})\pi, \pi^{-k} = (\pi^{-1})^k$ . 于是如果  $k$  是偶数,  $(1\ 2)^k = \varepsilon$ ; 如果  $k$  是奇数,  $(1\ 2)^k = (1\ 2)$ .

**注意** 在 (21.2) 的记法中, 当  $i = \nu_i$  时即略去  $i$ . 譬如 (21.4) 又写成  $\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$ .

$$\text{例2} \quad \begin{pmatrix} 1 & 2 & \dots & n \\ \mu_1 & \mu_2 & \dots & \mu_n \end{pmatrix} \begin{pmatrix} 1 & 2 & \dots & n \\ \nu_1 & \nu_2 & \dots & \nu_n \end{pmatrix} \begin{pmatrix} 1 & 2 & \dots & n \\ \mu_1 & \mu_2 & \dots & \mu_n \end{pmatrix}^{-1} = \begin{pmatrix} \mu_1 & \mu_2 & \dots & \mu_n \\ \mu_{\nu_1} & \mu_{\nu_2} & \dots & \mu_{\nu_n} \end{pmatrix}.$$

**例3** 假定  $S = \{1, 2\}$ , 那末  $\mathfrak{S}(S) = \{\varepsilon, (1\ 2)\}$ . 恒等映射  $\varepsilon$  也有写成 (1) 的。

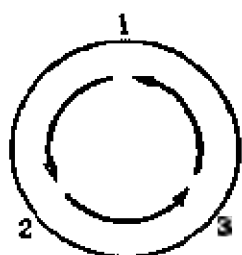


图 21.1

**例4** 置换  $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$  叫做 1, 2, 3 的**循环置换**, 用  $(1\ 2\ 3)$

表示。(同样  $(1\ 2\ 3 \dots k)$  表示  $\begin{pmatrix} 1 & 2 & \dots & k-1 & k \\ 2 & 3 & \dots & k & 1 \end{pmatrix}$ .) 当  $S = \{1, 2, 3\}$  时,  $\mathfrak{S}(S)$  是由下面六个元构成: (1), (1 2), (2 3), (1 3), (1 2 3), (1 3 2). 关于它们, 下面的关系成立:

$$(1\ 3)(1\ 2) = (1\ 2\ 3), (1\ 2\ 3)(1\ 3\ 2) = (1):$$

**例5** 当  $S = \{1, 2, 3, 4\}$  时,  $\mathfrak{S}(S)$  是由下面  $4! = 24$  个元构成:

$$(1), (1\ 2), (1\ 3), (1\ 4), (2\ 3), (2\ 4), (3\ 4),$$

$$(1\ 2\ 3) = (1\ 3)(1\ 2), (1\ 2\ 4) = (1\ 4)(1\ 2), (1\ 3\ 2) = (1\ 2)(1\ 3),$$

$$(1\ 3\ 4) = (1\ 4)(1\ 3), (1\ 4\ 2) = (1\ 2)(1\ 4), (1\ 4\ 3) = (1\ 3)(1\ 4),$$

$$(2\ 3\ 4) = (2\ 4)(2\ 3), (2\ 4\ 3) = (2\ 3)(2\ 4),$$

$$(1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3),$$

$$(1\ 2\ 3\ 4), (1\ 2\ 4\ 3), (1\ 3\ 2\ 4), (1\ 3\ 4\ 2), (1\ 4\ 2\ 3), (1\ 4\ 3\ 2).$$

假定对于  $G$  上  $n$  个变数的多项式 (21.1) 施行置换 (21.2), 那就得到

$$f(x_{\nu_1}, x_{\nu_2}, \dots, x_{\nu_n}) = \sum \alpha_{k_1 \dots k_n} x_{\nu_1}^{k_1} \dots x_{\nu_n}^{k_n}.$$

这事实用下式表示:

$$\pi(f(x_1, x_2, \dots, x_n)) = f(x_{\nu_1}, x_{\nu_2}, \dots, x_{\nu_n}). \quad (21.5)$$

例 6  $\pi(\pi(f(x_1, \dots, x_n))) = \pi \circ \pi(f(x_1, \dots, x_n)).$

例 7 对于  $f(x_1, x_2, x_3) = \alpha_1 x_1 + \alpha_2 x_2 + \alpha_3 x_3$  施行  $\mathfrak{S}(\{1, 2, 3\})$  中六个置换的结果如下:

$$\begin{aligned} (1) (f(x_1, x_2, x_3)) &= \alpha_1 x_1 + \alpha_2 x_2 + \alpha_3 x_3, \\ (1\ 2) (f(x_1, x_2, x_3)) &= \alpha_2 x_1 + \alpha_1 x_2 + \alpha_3 x_3, \\ (2\ 3) (f(x_1, x_2, x_3)) &= \alpha_1 x_1 + \alpha_3 x_2 + \alpha_2 x_3, \\ (1\ 3) (f(x_1, x_2, x_3)) &= \alpha_3 x_1 + \alpha_2 x_2 + \alpha_1 x_3, \\ (1\ 2\ 3) (f(x_1, x_2, x_3)) &= \alpha_3 x_1 + \alpha_1 x_2 + \alpha_2 x_3, \\ (1\ 3\ 2) (f(x_1, x_2, x_3)) &= \alpha_2 x_1 + \alpha_3 x_2 + \alpha_1 x_3. \end{aligned}$$

于是多项式 (21.1) 是对称式意指对  $f(x_1, \dots, x_n)$  施行  $\mathfrak{S}(S)$  的任意置换  $\pi$  而不改变, 即用

$$\pi(f(x_1, \dots, x_n)) = f(x_1, \dots, x_n), \quad \forall \pi \in \mathfrak{S}(S)$$

( $\forall \pi \in \mathfrak{S}(S)$  读成“对于  $\mathfrak{S}(S)$  中所有元  $\pi$ ”)来定义, (21.1) 是交代式意指  $f$  对于  $\mathfrak{S}(S)$  中任意对换  $(ij)$  只变符号, 用下式定义:

$$(ij)(f(x_1, \dots, x_n)) = -f(x_1, \dots, x_n).$$

例 8 在例 7 中,  $f(x_1, x_2, x_3)$  是对称式的必要充分条件是  $\alpha_1 = \alpha_2 = \alpha_3$ , 是交代式的必要充分条件是  $\alpha_1 - \alpha_2 = \alpha_3 = 0$ .

上面交代式的定义比对称式的定义也许感到不自然。但是它的必然性能够象下面那样来说明 (参照后面的命题 5)。

**命题 1**  $\mathfrak{S}(S)$  中任意元能够表示为几个对换的结合。

**证明** 用 62 页所示的方法也能够证明, 但在这里用关于  $S$  中元的个数的数学归纳法来证明。

假定  $S = \{1, 2\}$ , 那末  $\mathfrak{S}(S) = \{(1), (1\ 2)\}$ , 因为  $(1) = (1\ 2)(1\ 2)$ , 所以这时命题成立。

对于  $S = \{1, \dots, n-1\}$ , 假定命题成立, 来考虑  $S = \{1, 2, \dots, n\}$ ,

这时命  $\mathfrak{S}(S)$  中任意元

$$\pi = \begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ \nu_1 & \nu_2 & \cdots & \nu_{n-1} & \nu_n \end{pmatrix}.$$

如果  $\nu_n = n$ , 那末  $\pi = \begin{pmatrix} 1 & \cdots & n-1 \\ \nu_1 & \cdots & \nu_{n-1} \end{pmatrix} \in \mathfrak{S}(\{1, 2, \dots, n-1\})$ , 所以  $\pi$  能够表为对换的结合。如果  $\nu_n \neq n$ , 命  $\nu_k = n$ , 那末

$$\pi = (\nu_n \nu_k) \begin{pmatrix} 1, \dots, k-1, k, k+1, \dots, n-1, n \\ \nu_1, \dots, \nu_{k-1}, \nu_k, \nu_{k+1}, \dots, \nu_{n-1}, n \end{pmatrix},$$

所以还是能够表为对换的结合。

**系** 假如多项式  $f$  对于所有的对换不变, 那末  $f$  是对称式。

假如把 (21.5) 右边的多项式, 叫做对于  $f(x_1, \dots, x_n)$  施行置换  $\pi$  的“值”, 那末对由上定义的对称式施行  $\mathfrak{S}(S)$  中  $n!$  个置换时, 总是形成“等价”的多项式(所谓两多项式

$$\sum \alpha_{k_1 \dots k_n} x_1^{k_1} \cdots x_n^{k_n}, \quad \sum \beta_{k_1 \dots k_n} x_1^{k_1} \cdots x_n^{k_n}$$

等价是指对于所有的  $k_1, \dots, k_n$ ,

$$\alpha_{k_1 \dots k_n} = \beta_{k_1 \dots k_n},$$

即对应的系数相等)。于是作为对称式的“次简单的”多项式, 可以认为是施行  $\mathfrak{S}(S)$  中  $n!$  个置换时, 恰好只取两个值的多项式。这样的多项式暂时叫做“两值多项式”。

假定  $f$  是两值多项式,  $\pi(f)$  ( $\pi \in \mathfrak{S}(S)$ ) 所取的两值是  $f_1, f_2$  ( $f_1 \neq f_2$ ), 如果  $\varepsilon(f) = f_1$ , 由命题 1, 对于适当的对换  $\tau = (ij)$ , 必须  $\tau(f) = f_2$ . 今假定  $\mathfrak{S}_1 = \{\pi_1; \pi_1 \in \mathfrak{S}(S), \pi_1(f) = f_1\}$ ,  $\mathfrak{S}_2 = \{\pi_2; \pi_2 \in \mathfrak{S}(S), \pi_2(f) = f_2\}$ , 那末  $\varepsilon \in \mathfrak{S}_1, \tau \in \mathfrak{S}_2, \mathfrak{S}(S) = \mathfrak{S} = \mathfrak{S}_1 + \mathfrak{S}_2$ .

**命题 2**  $\mathfrak{S}_i$  有下列各性质:

- (i)  $\mathfrak{S}_1 \ni \pi_1 \Rightarrow \mathfrak{S}_1 \ni \pi_1^{-1}$ .
- (ii)  $\mathfrak{S}_1 \ni \pi_1, \pi'_1 \Rightarrow \mathfrak{S}_1 \ni \pi'_1 \circ \pi_1$ .

**证明** (i) 因为  $f_1 = f, \pi_1(f) = f_1$ , 所以  $\pi_1^{-1}(f) = \pi_1^{-1}(\pi_1(f))$

$\pi = (\pi_1^{-1} \circ \pi_1)(f) = s(f) = f_1$ . 因此  $\pi_1^{-1} \in \mathfrak{S}_1$ .

(ii)  $(\pi'_1 \circ \pi_1)(f) = \pi'_1(\pi_1(f)) = \pi'_1(f_1) = \pi'_1(f) = f_1$ , 所以  $\pi'_1 \circ \pi \in \mathfrak{S}_1$ .

**系** 設  $\pi_1 \in \mathfrak{S}_1$ , 則  $\pi_1(f_2) = f_2$ , 即  $\mathfrak{S}_1$  中元分别不变  $f_1, f_2$ .

**証明** 假定  $\pi_1(f_2) = f_1$ , 那末  $\pi_1^{-1}(f_1) = f_2$ , 这与命题 2 (i) 矛盾.

**命题 3**  $\mathfrak{S}_2$  中元对换  $f_1, f_2$ . 即假定  $\pi_2 \in \mathfrak{S}_2$ , 那末  $\pi_2(f_1) = f_2$ ,  $\pi_2(f_2) = f_1$ .

**証明**  $\pi_2(f_1) = f_2$  由  $\mathfrak{S}_2$  的定义自明. 又  $\pi_2(f_2) = f_1$  意味着  $\pi_2^{-1}(f_1) = f_2$ . 假如  $\pi_2^{-1}(f_1) = f_1$ , 由命题 2(i) 得  $\pi_2 \in \mathfrak{S}_1$ , 这与假设矛盾.

**例 9** (i)  $\mathfrak{S}_1 \ni \pi_1, \mathfrak{S}_2 \ni \pi_2 \Rightarrow \pi_1 \circ \pi_2 \in \mathfrak{S}_2, \pi_2 \circ \pi_1 \in \mathfrak{S}_2$ .

(ii)  $\mathfrak{S}_2 \ni \pi_2, \pi'_2 \Rightarrow \pi_2 \circ \pi'_2 \in \mathfrak{S}_1$ .

**例 10** 一般对于  $\mathfrak{S}$  的子集合  $\mathfrak{T}$  及  $\pi \in \mathfrak{S}$ , 假定

$$\{\pi \circ \pi; \pi \in \mathfrak{T}\}, \quad \{\pi \circ \pi; \pi \in \mathfrak{T}\}$$

分別用  $\pi \circ \mathfrak{T}, \mathfrak{T} \circ \pi$  表示, 那末  $\mathfrak{S}_2 = \tau \circ \mathfrak{S}_1 = \mathfrak{S}_1 \circ \tau$ .

**[解]**  $\tau \circ \mathfrak{S}_1 \subset \mathfrak{S}_2$  是明显的. 反之, 假如  $\pi \in \mathfrak{S}_2$ , 因为  $\tau\pi \in \mathfrak{S}_1, \tau^{-1} = \tau$ , 所以  $\pi = \tau(\tau\pi) \in \tau \circ \mathfrak{S}_1$ , 因此  $\mathfrak{S}_2 \subset \tau \circ \mathfrak{S}_1$ . 于是  $\mathfrak{S}_2 = \tau \circ \mathfrak{S}_1$ . 同样  $\mathfrak{S}_2 = \mathfrak{S}_1 \circ \tau$ .

**例 11** 对于任意  $\pi \in \mathfrak{S}$  有  $\pi \circ \mathfrak{S}_1 \circ \pi^{-1} = \mathfrak{S}_1$ .

**[解]** 假定  $\pi \in \mathfrak{S}_1$ , 那末  $\pi^{-1} \in \mathfrak{S}_1$ . 所以  $\pi \circ \mathfrak{S}_1 \circ \pi^{-1} \subset \mathfrak{S}_1$ . 同样  $\pi^{-1} \circ \mathfrak{S}_1 \circ \pi \subset \mathfrak{S}_1$ . 于是  $\mathfrak{S}_1 \subset \pi \circ \mathfrak{S}_1 \circ \pi^{-1}$ . 因此  $\pi \circ \mathfrak{S}_1 \circ \pi^{-1} = \mathfrak{S}_1$ .

假定  $\pi \in \mathfrak{S}_2$ , 因为  $\pi = \tau \circ \pi_1, \pi_1 \in \mathfrak{S}_1$ , 所以  $\pi \circ \mathfrak{S}_1 \circ \pi^{-1} = (\tau \circ \pi_1) \circ \mathfrak{S}_1 \circ (\pi_1^{-1} \circ \tau^{-1}) = \tau \circ (\pi_1 \circ \mathfrak{S}_1 \circ \pi_1^{-1}) \circ \tau^{-1} = \tau \circ \mathfrak{S}_1 \circ \tau^{-1} = \mathfrak{S}_2 \circ \tau^{-1} = \mathfrak{S}_1$ . 这最后的部分是根据例 10.

**例 12** 所有的对换属于  $\mathfrak{S}_2$ .

**[解]**  $\tau = (i \ j) \in \mathfrak{S}_2$ , 假如一个对换  $(k \ l) \in \mathfrak{S}_1$ , 由例 11,  $\begin{pmatrix} h & l \\ i & j \end{pmatrix} (k \ l) \begin{pmatrix} k & l \\ i & j \end{pmatrix}^{-1} = (i \ j) = \tau \in \mathfrak{S}_1$ , 这与假设不合.

**命题 4**  $f_1 + f_2$  是对称式,  $f_1 - f_2$  是交代式.

**証明** 假如  $\pi_1 \in \mathfrak{S}_1$ , 那末  $\pi_1(f_1 + f_2) = f_1 + f_2$ . 假如  $\pi_2 \in \mathfrak{S}_2$ ,

那末  $\pi_2(f_1+f_2)=f_2+f_1=f_1+f_2$ . 所以对于  $\mathfrak{S}$  中任意元  $\pi$ ,  $\pi(f_1+f_2)=f_1+f_2$ , 因此  $f_1+f_2$  是对称式。

又假如  $\pi_2 \in \mathfrak{S}_2$ , 那末  $\pi_2(f_1-f_2)=f_2-f_1=-(f_1-f_2)$ , 因此  $f_1-f_2$  由  $\mathfrak{S}_2$  中任意元只改变符号。因为对换都属于  $\mathfrak{S}_2$ , 于是  $f_1-f_2$  由任意对换只改变符号。所以它是交代式。

**系** 任意两值多项式能够表为对称式  $\frac{f_1+f_2}{2}$  与交代式  $\frac{f_1-f_2}{2}$  的和。

在交代式中,

$$p(x_1, \dots, x_n) = \prod_{i < j} (x_i - x_j)$$

叫做  $x_1, \dots, x_n$  的**最简交代式**。对于  $x_j, \dots, x_n$  的任意交代式  $g(x_1, \dots, x_n)$ ,  $(ij)(g) = -g$ , 即

$$g(x_1, \dots, x_j, \dots, x_i, \dots, x_n) = -g(x_1, \dots, x_i, \dots, x_j, \dots, x_n),$$

因此如果  $x_i = x_j$ , 那末  $g=0$ . 于是由剩余定理,  $g$  能够用  $(x_i - x_j)$  除尽。因为这对于  $i, j$  的任何组合都成立, 所以  $g$  能够用最简交代式  $p$  除尽, 因而有适合  $g = ph$  的多项式  $h$ . 显然  $h$  是对称式。由命题 4 的系及这事实得下面的命题。

**命题 5** 任意两值多项式  $f$  能用适当的对称式  $f_0, h$  及最简单交代式  $p$  写成  $f_0 + ph$  的形状。

由以上的讨论可以了解交代式特别是最简交代式的意义。又如所周知, 任意对称式能够表为所谓**基本对称式**

$$\sum_{i=1}^n x_i, \quad \sum_{i < j} x_i x_j, \quad \sum_{i < j < k} x_i x_j x_k, \quad \dots, \quad x_1 x_2 \cdots x_n \quad (21.6)$$

的多项式。因此任意两值多项式能够表为这  $n$  个式与最简交代式  $p$  的多项式。

根据上面的事实, 熟知的二次方程的解法能够如下地说明。

假定二次方程  $x^2 + ax + b = 0$  的根是  $x_1, x_2$ , 那末  $x^2 + ax + b = (x - x_1)(x - x_2)$ , 于是

$$-a = x_1 + x_2, \quad b = x_1 x_2$$

是  $x_1, x_2$  的基本对称式。命  $f(x_1, x_2) = x_1$ , 那末它是  $x_1, x_2$  的二值多项式。于是由上述事实能够用对称式  $f_0, h$  与  $p(x_1, x_2) = x_1 - x_2$  表示  $x_1 = f_0 + ph$ . 用上面记法, 因为  $f_1 = x_1, f_2 = (1 \ 2)(f) = x_2$ , 所以

$$f_0 = \frac{1}{2}(f_1 + f_2) = \frac{x_1 + x_2}{2} = -\frac{a}{2}, \quad ph = \frac{f_1 - f_2}{2} = \frac{x_1 - x_2}{2} = \frac{p}{2}.$$

因为  $p$  的平方是对称式, 所以它也应当能够用  $a, b$  表示。实际上,  $p^2 = (x_1 - x_2)^2 = a^2 - 4b$ , 因此

$$x_1 = \frac{-a \pm \sqrt{a^2 - 4b}}{2},$$

这就是所熟知的二次方程的根的公式。

Lagrange 用同样的方法说明三次、四次方程的解法, 但对五次方程的解法杳无结果。一般五次方程的“代数的解法”为不可能的事实是在 1826 年由 Abel 所证明。象上面那样, 对于以根作变数的多项式或表示为其商的有理式研究施行“根的置换”后所引起的结果, 自 Lagrange 时代起已经流行, Abel “不可能的证明”也是根据这方法(参照高木贞治: 代数学讲义)。把它作为一般化的理论体系的是 Galois. 在这里不能详细介绍 Galois 的理论(参照正田, 浅野: 代数学 I), 但引入它的基础(key-word)置换群的概念来描述它的轮廓。

把  $n$  作为自然数,  $n$  个东西——它用数字  $1, 2, \dots, n$  表示——的集合  $S$  的置换(即自  $S$  到  $S$  上的全单射)全体的集合用  $\mathfrak{S}(S) = \mathfrak{S}$  表示。 $\mathfrak{S}$  的子集合  $\mathfrak{G}$  具有下面性质 (i), (ii), (iii) 时,  $\mathfrak{G}$  叫做  $S$  的置换群。

(i)  $\mathfrak{G} \ni \varepsilon$  ( $S$  的恒等映射)。

(ii)  $\mathfrak{G} \ni \pi \Rightarrow \mathfrak{G} \ni \pi^{-1}$ .

(iii)  $\mathfrak{G} \ni \pi_1, \pi_2 \Rightarrow \mathfrak{G} \ni \pi_1 \circ \pi_2$ .

**例 13** 假定  $\mathcal{G}$  不是空集, 由性质 (ii), (iii) 能够导出 (i)。

[解] 假定  $\pi \in \mathcal{G}$ , 由 (ii) 得  $\pi^{-1} \in \mathcal{G}$ , 因此由 (iii) 得  $\mathcal{G} \ni \pi \circ \pi^{-1} = \varepsilon$ 。

**例 14**  $\mathcal{G}$  自身及只由恒等置换  $\varepsilon$  形成的集合  $\{\varepsilon\}$  都是置换群。又在命题 2 之前定义的  $\mathcal{G}_1$  是置换群。关于一般的置换群  $\mathcal{G}$  总是  $\mathcal{G} \supset \mathcal{G}_1 \supset \{\varepsilon\}$ 。 $\mathcal{G}$  叫做  $S$  的对称群,  $\{\varepsilon\}$  叫做恒等群。 $\mathcal{G}_1$  是不使  $n$  个变数的两值多项式变动的置换形成的群。假如“不使两值多项式变动”用“不使交代式或最简交代式变动”来代替(由命题 5), 那末  $\mathcal{G}_1$  就叫做  $S$  的交代群。

**例 15** 置换作为对换的积表示时, “因子”对换的个数是偶数时, 这样的置换叫做偶置换, 是奇数时这样的置换叫做奇置换(这里奇偶性不论“因子分解”的方法如何总是一定的, 因此这定义与 62 页的定义一致)。交代群是由偶置换的全体构成的。

[解]  $n$  个变数的最简交代式  $p$ , 显然对偶置换不变, 而对奇置换变为  $-p$ ①。假定  $\pi \in \mathcal{G}$ , 因为  $\pi(p)$  为  $p$  或  $-p$  两者必属其一, 所以  $\pi$  的奇偶是一定的。因为对换都属于  $\mathcal{G}_2$ , 由例 9,  $\mathcal{G}_1$  与偶置换的全体一致。

一般, 假如给定  $n$  个变数的多项式  $f$  时, 那末不使  $f$  变动的这样置换的集合显然成为置换群。多项式或有理式的集合  $\{f, g, \dots\}$  已给定时, 使  $f, g, \dots$  都不变动的置换的集合也显然成为置换群。反之, 对于给定的某置换群, 可以来考虑由它不变动的多项式或有理式的集合。

Galois 的思想如下。

解以  $x_1, \dots, x_n$  为根的  $n$  次方程

$$\begin{aligned} \textcircled{1} \quad p = & \prod_{1 \leq i < j \leq n} (x_i - x_j) = (x_{n-1} - x_n) \\ & \cdot (x_{n-2} - x_n) (x_{n-2} - x_{n-1}) \cdots \\ & \cdots \cdots \cdots \\ & \cdot (x_1 - x_n) (x_1 - x_{n-1}) \cdots (x_1 - x_2), \end{aligned}$$

可以写成

$$p = (x_k - x_l) \pi(x_i - x_k) (x_l - x_l) F, \quad i \neq k, l$$

这里  $F$  不含有  $x_k$  及  $x_l$ 。现在假设在  $p$  上施行对换  $(x_k x_l)$ , 因为  $F$  及  $(x_i - x_k) (x_l - x_l)$  都不变而  $(x_k - x_l)$  变了符号, 所以  $p$  就换成  $-p$  了。这就是说在  $p$  上施行一个对换,  $p$  就变了符号, 因此假如用偶数个对换在  $p$  上继续施行, 结果仍然是  $p$ , 假如用奇数个对换在  $p$  上继续施行, 结果就是  $-p$ 。——译者注

$$x^n + a_1 x^{n-1} + \cdots + a_n = (x - x_1) \cdots (x - x_n) \quad (21.7)$$

不外是用系数  $a_1, \cdots, a_n$  表出根  $x_1, \cdots, x_n$ . 但  $a_1, \cdots, a_n$  除符号外与  $x_1, \cdots, x_n$  的基本对称式 (21.6) 一致。“表出”根时, 在所谓代数的解法中, 所用的是加减乘除的四则运算与开方。因为四则运算是代数学中最基本的算法, 所以便于把“四则运算能够如常施行的范围”看成为一个东西——这样就产生了“体的概念”。自复数体  $C$  出发, 解 (21.7) 的问题归结于自含  $C$  及  $a_1, \cdots, a_n$  (或  $C$  及  $x_1, \cdots, x_n$  的基本对称式 (21.6)) 的体  $K_0$  出发来求出——根据某些方法——含  $C$  及  $x_1, \cdots, x_n$  的体  $K$  的问题。因为  $K_0$  中元都是  $x_1, \cdots, x_n$  的对称式 (多项式或有理式), 所以对于对称群  $\mathfrak{S}$  不变。由此用某个“代数方法”求出“ $n$  值多项式”  $f(x_1, \cdots, x_n) = x_i$  即可。Galois 的基本思想是对于自  $K_0$  到达  $K$  的“代数方法”的阶段, 有  $K$  的子体列

$$K_0 \subset K_1 \subset K_2 \subset \cdots \subset K_r = K$$

与之对应。而对于这, 又有置换群列

$$\mathfrak{S} = \mathfrak{S}_0 \supset \mathfrak{S}_1 \supset \mathfrak{S}_2 \supset \cdots \supset \mathfrak{S}_r = \{\varepsilon\}$$

与之对应, 这时  $K_i$  正好是对于  $\mathfrak{S}_i$  不变的有理式的集合。根据这个思想, 方程的“代数解法”的问题归结到对称群的构造的问题, Abel 定理乃作为其一般理论之极特殊情况导出。

Galois 理论的说明不得不止于此, 在这里所用的“使某些东西——在上面是多项式或有理式——不变的置换群”的概念是重要的。但是只考虑置换群实嫌过窄, 因此有必要来考虑更一般的“变换群”。

置换定义为自有限集合  $S$  到它自身上的全单射。一般任意集合  $S$  (也叫做“空间”, 不是有限也可) 到它自身上的全单射叫做  $S$  的**正则变换**。 $S$  的正则变换全体的集合用  $\mathfrak{S}(S)$  表示。 $S$  的两个变换  $\pi_1: S \rightarrow S$ ,  $\pi_2: S \rightarrow S$  能够按照 § 6 的意义结合, 它的结果  $\pi_1 \circ \pi_2$



或  $\pi_2 \circ \pi_1$  又是  $S$  的变换。特别, 假如  $\pi_1, \pi_2 \in \mathfrak{S}(S)$ , 显然  $\pi_1 \circ \pi_2, \pi_2 \circ \pi_1 \in \mathfrak{S}(S)$ .  $\mathfrak{S}(S)$  的子集合  $\mathfrak{G}$  满足与上面 (i), (ii), (iii) 同样的条件时,  $\mathfrak{G}$  叫做变换群。置换及置换群不过是当  $S$  为有限时, 正则变换及变换群的特例。

**例 16**  $\mathfrak{S}(S)$  全体及  $\{\varepsilon\}$  ( $\varepsilon$  是  $S$  的恒等映射) 都是变换群。在一般情况,  $\mathfrak{S}(S), \{\varepsilon\}$  也分别叫做  $S$  的对称群, 恒等群。

**例 17** 假定  $S = \mathbf{R}$  (实数体),  $\pi \in \mathfrak{S}(\mathbf{R})$ , 对于  $\mathbf{R}$  中任意两元  $x, y$ , 如果  $\pi(x) - \pi(y) = x - y$ , 那就有  $\mathbf{R}$  中常数  $a \in \mathbf{R}$  使  $\pi(x) = x + a$ , 这  $\pi$  假定用  $\pi_a$  表示, 那末  $\pi_a \circ \pi_b = \pi_{a+b} = \pi_b \circ \pi_a, \pi_a^{-1} = \pi_{-a}$ . 于是  $\{\pi_a; a \in \mathbf{R}\}$  成为  $\mathbf{R}$  的变换群。它叫做  $\mathbf{R}$  的平行移动群。

[解] 命  $\pi(0) = a$ , 那末  $\pi(x) - a = x$ , 所以  $\pi(x) = x + a$ .

上例  $\mathbf{R}$  的平行移动群是“不使两元之差变动的  $\mathbf{R}$  的变换群”。不变我们现实空间中一点  $O$  (即不使  $O$  变动) 的变换全体成为绕  $O$  的旋转群, 不变两点间距离的变换全体成为空间的运动群。一般, 不变  $S$  的子集合的某性质的变换全体的集合成为  $S$  的一个变换群。

反之, 设已给定空间  $S$  的一个变换群  $\mathfrak{G}$ , 对于  $S$  的两个子集合  $A, A'$ , 假如  $\mathfrak{G}$  中存在元  $\pi$  使  $\pi(A) = A'$ , 那末  $A, A'$  叫做关于  $\mathfrak{G}$  相合, 写成  $A \equiv A'(\mathfrak{G})$ . 这样定义的相合关系, 显然是等价关系 (§4)。又“相合集合的共通性质”能够看成为“对于  $\mathfrak{G}$  不变的性质”。Klein 根据这思想把几何来分类 (Erlanger Programm, 1872). 譬如 Euclid 几何学是研究对于运动群不变的图形的性质, 非 Euclid 几何学是研究对于叫做“非 Euclid 运动群”的变换群不变的图形的性质等等, 关于此, 在这里不能详述。但它也可以根据与 Galois 理论同样的思想来理解。

**例 18** 在空间内的正三角形与它自身重合的运动成为与  $\mathfrak{S}(\{1, 2, 3\})$  同构的变换群。

[解] 由这样的一个运动  $\alpha$ , 正三角形的三顶点 1, 2, 3 分别与顶点  $\alpha$ ,

$\beta, \gamma$  重合时, 对于  $x$  使  $\begin{pmatrix} 1 & 2 & 3 \\ \alpha & \beta & \gamma \end{pmatrix} \in \mathcal{G}(\{1, 2, 3\})$  对应即可。

**注意** 一般在空间内的图形——结晶, 花纹等——重合于它自身的运动成为空间的变换群。这变换群可以看成为这图形对称性的表示。

特别, 图形是正多面体时, 把它重合于它自身的运动的群叫做多面体群。因为正多面体有正四面体, 正六面体 (= 立方体), 正八面体, 正十二面体, 正二十面体 5 种, 所以应该有 5 种多面体群。但连结正六面体各面的中心时, 即得正八面体, 连结正十二面体各面的中心时, 即得正二十面体, 所以正六面体与正八面体, 正十二面

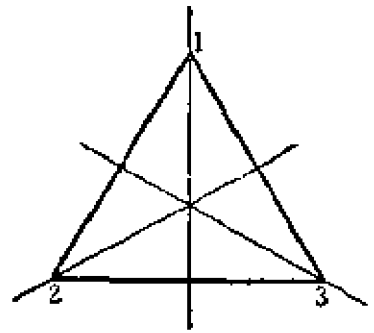


图 21.2

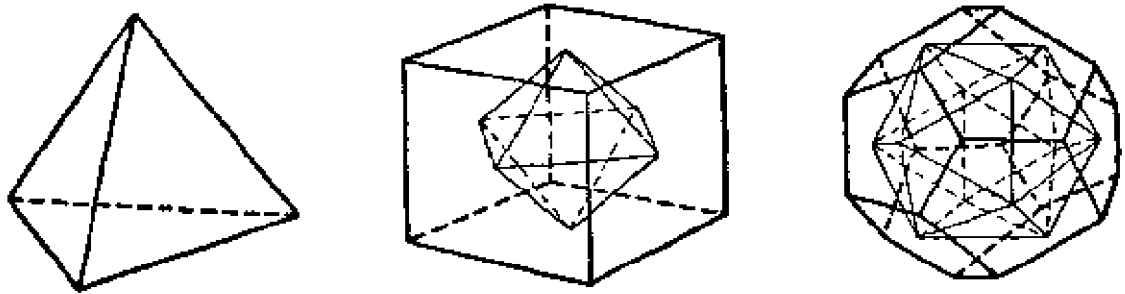


图 21.3

体与正二十面体, 其重合于它自身的群分别同构。因此多面体群有正四面体群, 正八面体群, 正二十面体群 3 种。它们是分别与四次交代群, 四次对称群, 五次交代群同构的<sup>①</sup>。(关于同构的详细定义请参照下节。)

## § 22 群

作为代数系的群可以用可换群的公理  $A^\circ 1 \sim 5$  (§ 3), 而只除去其中的交换律  $A^\circ 2$  来定义。为慎重起见, 将它重写一下, 那就是

$A^\circ 1$  假定  $G$  是非空集合, 对于  $x, y \in G$ , 给定了使  $G$  中元  $x \circ y$  唯一对应的算法。

$A^\circ 3$   $(x \circ y) \circ z = x \circ (y \circ z)$  (结合律)。

$A^\circ 4$  对于  $G$  中任意元  $x$ ,  $G$  中存在满足  $x \circ \theta = \theta \circ x = x$  这样的

① 参阅附录“有限旋转群”。——译注者

一元  $e$  ( $e$  叫做  $G$  的单位元)。

A°5 对于  $x \in G$ , 存在满足  $x' \circ x = x \circ x' = e$  这样的  $x' \in G$  ( $x'$  叫做  $x$  的逆元)。

这时  $G$  叫做关于算法  $\circ$  成群。变换群 (把映射的褶合作为算法  $\circ$ ——因为映射的褶合服从结合律——) 一定是群。又可换群当然是群。为了简化算法的记法, 代替上面的  $x \circ y$  多写成  $xy$ ——积的形式。今后若不预先声明, 群的算法都表为这种形状。

用这种记法时, 群  $G$  的基本算法是“乘法”与“作逆元的算法”。对于  $G$  的元  $a$  及两个子集合  $X, Y$ , 命

$$aX = \{ax; x \in X\}, \quad Xa = \{xa; x \in X\},$$

$$XY = \{xy; x \in X, y \in Y\}, \quad X^{-1} = \{x^{-1}, x \in X\}.$$

假如  $H (\neq \emptyset) \subset G$  满足  $HH^{-1} \subset H$ , 那末  $H$  叫做“关于群算法是 (封) 闭的”。这时  $H$  关于与  $G$  同样的算法显然成群。它叫做  $G$  的子群。

例 1 (i)  $HH^{-1} \subset H \neq \emptyset \Rightarrow HH^{-1} = H$ .

(ii)  $HH^{-1} \subset H \Leftrightarrow HH \subset H, H^{-1} \subset H$ .

[解] (i) 假定  $e \in H$ , 那末  $e = x_0 x_0^{-1} \in H$ . 如果  $x$  是  $H$  中任意元, 那末  $x = xe = xe^{-1} \in HH^{-1}$ . 所以  $H \subset HH^{-1}$ .

(ii)  $H = \emptyset$  时是明显的。考虑  $H \neq \emptyset$  的情况。假如  $HH^{-1} \subset H$ , 由 (i)  $e \in H$ , 所以  $H^{-1} = eH^{-1} \subset HH^{-1} \subset H$ . 如果  $xy (x \in H, y \in H)$  是  $HH$  中任意元, 由  $y \in H$ , 得  $y^{-1} \in H$ , 所以  $xy = x(y^{-1})^{-1} \in HH^{-1} \subset H$ . 于是  $HH \subset H$ . 反之, 假如  $HH \subset H, H^{-1} \subset H$ , 那末  $HH^{-1} \subset HH \subset H$ .

注意 在 §3 曾就一般代数系的子系。同态映射, 同构映射等作了阐述。子群不外是作为代数系的群子系。关于以下所述的群的生成, 同态, 同构, 直积等, 也都适合于作为代数系一般概念的群。

假如群  $G$  有子集合  $M$ , 那末在  $G$  中唯一存在含  $M$  的最小子群, 此可与 §3 命题 2 同样证明。它叫做由  $M$  生成的子群, 用  $[M]$  表示。

假如有两个群  $G_1, G_2$  与自  $G_1$  到  $G_2$  上的映射  $f: G_1 \rightarrow G_2$ , 如果  $f$  保存  $G_1$  的基本算法, 即如果  $f(xy^{-1}) = f(x)(f(y))^{-1}$ , 那末  $f$  叫做自  $G_1$  到  $G_2$  的同态映射。当自  $G_1$  到  $G_2$  上的同态映射存在时,  $G_2$  叫做同态于  $G_1$ , 同态映射是全单射的叫做同构映射。自  $G_1$  到  $G_2$  的同构映射存在时,  $G_1$  叫做同构于  $G_2$ , 记为  $G_1 \cong G_2$ , 同构关系显然是等价关系(同构这名词在 § 21, 例 18 也用过)。

假如有  $k$  个群  $H_1, \dots, H_k$ , 它们的群的直积  $G = H_1 \otimes \dots \otimes H_k = \prod_{i=1}^k \otimes H_i$  (与向量空间直积的情况一样) 定义如下:

$G$  中元是集合  $H_i$  的直积  $H_1 \times \dots \times H_k$  中元  $(x_1, \dots, x_k)$  ( $x_i \in H_i$ ), 其中两元  $x = (x_1, \dots, x_k), y = (y_1, \dots, y_k)$  之间的基本算法假定是

$$xy = (x_1 y_1, \dots, x_i y_i, \dots, x_k y_k), \quad x^{-1} = (x_1^{-1}, \dots, x_k^{-1}).$$

那末  $G$  显然成为群。 $e_i$  是  $H_i$  的单位元时,

$$e = (e_1, \dots, e_k)$$

是  $G$  的单位元。这时  $(e_1, \dots, e_{i-1}, x_i, e_{i+1}, \dots, e_k)$  ( $x_i \in H_i$ ) 形状的元形成与  $H_i$  同构的  $G$  的子群。假如把它看成  $H_i$ , 它的元仍旧用  $x_i$  表示, 那末  $G$  中任意元能够唯一地表示为  $x_1 x_2 \dots x_k$  ( $x_i \in H_i$ ) 的形状。这时  $i \neq j \Rightarrow x_i x_j = x_j x_i$ 。反之, 假如  $H_i$  ( $i = 1, \dots, k$ ) 是  $G$  的子群, 当  $i \neq j$  时  $H_i$  中元与  $H_j$  中元可换,  $G$  中任意元能够唯一地写成  $x_1 x_2 \dots x_k$  ( $x_i \in H_i$ ) 的形状, 那末  $G$  成为(同构于)  $H_i$  的直积。群的基本算法不用积的形状而写成和的形状时, 直积就用直和这名词来代替,  $H_1 \otimes \dots \otimes H_k$  的记法也就用  $H_1 \oplus \dots \oplus H_k$ 。

我們已經知道变换群与可换群, 虽然群的例子已不少, 但不妨再示下面数例。

**例 2** 当  $V$  是体  $K$  上向量空间时,  $V$  的正则线性变换(即自  $V$  到  $V$  自身的线性映射是全单射的) 全体的集合形成把映射的褶合作为算法的群, 叫做  $V$  的一般线性变换群, 用  $GL(V)$  表示 ( $GL$  是 General Linear 之略)。

**例3** 当  $\dim V = n$  时, 假如取  $V$  的坐标  $\varphi$ , 那末  $GL(V)$  中元能够用体  $K$  上  $n$  级正则矩阵表示。  $K$  上  $n$  级正则矩阵全体的集合形成关于矩阵乘法的群。它用  $GL(n, K)$  表示。显然  $GL(V) \cong GL(n, K)$ 。

**例4**  $GL(V)$  是由作为代数系的  $V$  的自同构的全体形成的群。不论是如何的代数系, 它的自同构的全体也形成把映射的褶合作为算法的群。它叫做代数系的自同构群。

**例5** 假定  $V$  是  $n$  维 Euclid 空间, 那末  $V$  的直交变换的全体形成  $GL(V)$  的子群, 叫做  $V$  的直交变换群。  $n$  级直交矩阵的全体形成与它同构的群, 它用  $O(n, R)$  表示。  $O(n, R)$  是  $GL(n, R)$  的子群。特征直交矩阵的全体又形成  $O(n, R)$  的子群, 它用  $O^+(n, R)$  表示。

**例6** 当  $A$  是体  $K$  上  $n$  级对称矩阵时,  $GL(n, K)$  中使  $TA^*T = A$  这样 (使  $A$  不变的) 的元  $T$  形成  $GL(n, K)$  的子群。  $K = R, A = E$  时, 这子群不外是  $O(n, R)$ 。在  $K = R, n = 4, A = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$  时, 这子群叫做 Lorentz 群。

**例7** 与例5同样能够定义  $n$  阶酉变换群与表示它的  $n$  级酉矩阵群  $U(n, C)$ 。

**例8** 体  $K$  中元关于加法成为可换群,  $K - \{0\} = K^*$  关于乘法成为可换群。这由体的公理 (C, §3) 自明。这些群叫做  $K$  的加法群, 乘法群。它仍旧用  $K, K^*$  表示。特别,  $R, R^*, C, C^*$  分别叫做实数的加法群, 乘法群, 复数的加法群, 乘法群。这时  $C = R \oplus R$ 。正实数全体关于乘法也成为可换群, 它用  $R^+$  表示, 于是  $R^+$  是  $R^*$  的子群。加法群  $R$  与乘法群  $R^+$  同构。假如  $y = \exp x = f(x)$ , 那末  $f: R \rightarrow R^+$  给出自  $R$  到  $R^+$  的同构映射,  $x = \log y = g(y)$  给出它的逆映射  $g: R^+ \rightarrow R$ 。又对于  $z \in R^*$  或  $z \in C^*, z \rightarrow |z|$ , 给出自  $R^*$  或  $C^*$  到  $R^+$  的同态映射。

**例9** 由两个实数  $1, -1$  构成的集合  $\{1, -1\}$ , 关于乘法成群, 是  $R^*$  的子群, 它与二阶对称群  $\mathfrak{S}(\{1, 2\})$  同构。  $R^* \ni z \rightarrow \frac{z}{|z|}$  给出自  $R^*$  到  $\{1, -1\}$  的同态映射。又  $R^*$  能够用  $R^+$  与  $-1$  生成。再, 绝对值是1的复数的集合, 作成  $C^*$  的子群。用  $U$  表示。  $U$  与  $O^+(2, R)$  同构。  $C^* \ni z \rightarrow \frac{z}{|z|} \in U$  给出自  $C^*$  到  $U$  的同态映射。  $C^*$  能够用  $U$  与  $R^+$  生成。

**例10** 有理整数  $\cdots, -3, -2, -1, 0, 1, 2, 3, \cdots$  关于加法成群。它用

$\mathbf{Z}$  表示。 $\mathbf{Z}$  是加法群  $R$  的子群。假定  $m \in \mathbf{Z}$ ,  $m \neq 0$ , 对于  $x, x' \in \mathbf{Z}$ ,  $x - x'$  是  $m$  的倍数时, 写成  $x \equiv x' \pmod{m}$ , 叫做  $x, x'$  对于  $\text{mod } m$  相合, 这相合关系显然是等价关系。因此  $x \equiv x' \pmod{m}$  时,  $x, x'$  叫做关于  $\text{mod } m$  属于相同的剩余类, 写成  $(x)_m = (x')_m$ . 当  $m$  固定时, 也可省略  $(x)_m$  的  $m$  及相合式的  $\pmod{m}$ . 显然  $x \equiv x', y \equiv y' \Rightarrow x + y \equiv x' + y'$ , 所以把  $(x + y)$  命名为  $(x)$  与  $(y)$  的和是可以的。对于这种“加法”, 关于  $\text{mod } m$  的剩余类  $(0), (1), (2), \dots, (m-1)$  形成可换群。这群用  $\mathbf{Z}_m$  表示。 $\mathbf{Z}_m$  与  $\mathfrak{S}(\{1, 2, \dots, m\})$  中用循环置换  $(1, 2, \dots, m)$  生成的子群同构。与  $\mathbf{Z}_m$  同构的群, 叫做  $m$  阶循环群。与  $\mathbf{Z}$  同构的群, 也叫做无限阶循环群。用有限个元生成的可换群, 是若干个无限阶或有限阶的循环群的直积(可换群的基本定理)①。

上面给出群的很多具体例子。由有限集合形成的群叫做有限群。象它们之中的: 恒等群, 例 9 的  $\{1, -1\}$ , 例 10 的  $\mathbf{Z}_m$  或  $\mathfrak{S}(\{1, 2, \dots, m\})$  及其的子群等, 不是有限的 ( $\mathbf{Z}, R, R^*, C, C^*, GL(n, R)$  等) 叫做无限群。有限群中元的个数叫做群的阶。在讨论  $GL(n, R)$  和它的子群时, 引入它的拓扑而作为所谓拓扑群来讨论, 常较方便。但在这里已没有机会深入到这方面了(请参阅本丛书中的“李群论”)。

把例 10 的思想一般化, 遂得到下述的定理, 它虽简单, 但极重要。

**定理 1** 假定  $G$  是群,  $H$  是它的子群, 那末对于  $x, y \in G$ , 下面的六个条件是等价的:

- |                       |                                      |
|-----------------------|--------------------------------------|
| (i) $xy^{-1} \in H$ , | (i') $yx^{-1} \in H$ ,               |
| (ii) $Hx \supset y$ , | (ii') $Hy \supset x$ ,               |
| (iii) $Hx = Hy$ ,     | (iii') $Hx \cap Hy \neq \emptyset$ . |

**证明** (i)  $\Leftrightarrow$  (i'). 假定  $xy^{-1} \in H$ , 那末  $yx^{-1} = (xy^{-1})^{-1} \in H$ . 反之是同样的。

① 参阅 E. 阿丁著“伽罗华理论”, II. 体论, I. 有限体。李英译, 上海科学技术出版社。——译者注

(i)  $\Leftrightarrow$  (ii'). 假定  $xy^{-1} \in H$ , 那末  $Hy \ni (xy^{-1})y = x$ . 反之, 假定  $Hy \ni x$ , 那末  $xy^{-1} \in (Hy)y^{-1} = H$ .

(i')  $\Leftrightarrow$  (ii). 能够与上同样证明。

于是 (i), (i'), (ii), (ii') 等价。

(i)  $\Rightarrow$  (iii). 假定 (i) 成立, 因为 (ii) 成立, 所以能够写成  $y = hx (h \in H)$ . 于是, 如果  $h' \in H$ , 那末  $h'y = h'hx \in Hx$ . 所以  $Hy \subset Hx$ . 又因为 (ii') 也成立. 同样,  $Hx \subset Hy$ . 因此  $Hx = Hy$ .

(iii)  $\Rightarrow$  (iii'). 显然。

(iii')  $\Rightarrow$  (i). 假定  $z \in Hx \cap Hy$ , 那末,  $z = h_1x = h_2y (h_1, h_2 \in H)$ , 所以  $xy^{-1} = h_1^{-1}h_2 \in H$ .

由以上 (iii), (iii') 也与 (i) 等价。 (証毕)

$G$  的子集合  $Hx$  叫做  $x$  关于  $\text{mod } H$  的右剩余类。当定理 1 的六个条件中任一个 (因此所有) 成立时, 写成  $x \equiv y \pmod{H}$ . 这关系显然是等价关系。今于  $G$  的子集合  $\{x_\alpha\}$ , 假定  $\alpha \neq \alpha'$  时即不得有  $x_\alpha \equiv x_{\alpha'} \pmod{H}$ , 并且对于  $G$  中任意元  $x$  有适当的  $\alpha$  存在使  $x \equiv x_\alpha \pmod{H}$ , 那末  $G$  成为  $Hx_\alpha$  作为集合的直和

$$G = \sum_{\alpha} Hx_{\alpha}, \quad (22.1)$$

它叫做  $G$  关于  $\text{mod } H$  的右剩余系的分解。与这完全同样, 能够定义  $G$  关于  $\text{mod } H$  的左剩余系的分解

$$G = \sum_{\beta} y_{\beta}H. \quad (22.1')$$

**例 11** 假定  $G = \mathfrak{S}(\{1, 2, 3\})$ ,  $H = \{(1), (1\ 2)\}$ , 那末

$$G = H + H(1\ 3) + H(2\ 3),$$

这里  $H(1\ 3) = \{(1\ 3), (1\ 3\ 2)\}$ ,  $H(2\ 3) = \{(2\ 3), (1\ 2\ 3)\}$ ;

$$G = H + (1\ 3)H + (2\ 3)H,$$

这里  $(1\ 3)H = \{(1\ 3), (1\ 2\ 3)\}$ ,  $(2\ 3)H = \{(2\ 3), (1\ 3\ 2)\}$ .

特别,  $G$  是阶为  $g$  的有限群时, 假定  $H$  的阶是  $h$ ,  $\{x_\alpha\}$  中元的个数是  $k$ , 由 (22.1) 得

$$g = hk.$$

假定  $\{y_{k'}\}$  中元的个数是  $k'$ , 由 (22.1') 得

$$g = hk'.$$

所以  $k = k' = g/h$ . 这  $k$  叫做  $H$  关于  $G$  的指数, 记为  $(G:H)$  (因而单位群若用 1 表示, 则群的阶是  $(G:1)$ ). 由上式得

**定理 2** (Lagrange) 有限群  $G$  的子群的阶是  $G$  的阶的约数。

由这定理更导出下面的事实。

假定  $x$  是有限群  $G$  中元,  $G$  中用  $x$  生成的子群  $H$  显然是具有  $\{e, x, x^2, \dots, x^{m-1}\}$  形状的循环群。这时  $x^m = e$ .  $H$  的阶  $m$  也叫做  $x$  的阶。由定理 2,  $x$  的阶  $m$  是  $G$  的阶  $g$  的约数。于是  $x^g = x^{m(g/m)} = e$ . 因此得下面的定理 2 的系。

**定理 2 的系** 假定  $x$  是有限群  $G$  中任意元,  $g$  是  $G$  的阶, 那末  $x^g = e$  (单位元)。 (系毕)

$H$  是  $G$  的子群时,  $x$  关于  $\text{mod } H$  的左剩余类  $xH$  与右剩余类  $Hx$  不一定一致。假如对于任意  $x \in G$ , 总是

$$xH = Hx, \text{ 即 } xHx^{-1} = H$$

时, 那末,  $H$  叫做  $G$  的**正规子群**。假如  $H$  是  $G$  的正规子群, 那末对于任意  $x, y \in G$ ,

$$Hx \cdot Hy^{-1} = H \cdot x \cdot Hy^{-1} = H \cdot Hx \cdot y^{-1} = Hxy^{-1}.$$

于是, 对于  $x \in G$ , 使与  $x$  关于  $\text{mod } H$  的剩余类 (当  $H$  是正规子群时, 没有必要区别剩余类的左右)  $Hx$  对应, 就得到同态于  $G$  的群, 这群叫做  $G$  对于正规子群  $H$  的商群, 用  $G/H$  表示。又对于  $x \in G$ , 使与  $Hx \in G/H$  对应的映射, 叫做自  $G$  到  $G/H$  的**自然映射**。这事实的逆, 就是下面的重要定理。

**定理 3** 假定  $G'$  是同态于  $G$  的群,  $f$  是自  $G$  到  $G'$  上的同态映射。这时  $G'$  的单位元如果是  $e'$ , 那末  $H = \{x; f(x) = e'\}$  是  $G$  的正规子群,  $G' \cong G/H$  (同态定理)。



**証明** (i) 首先示  $H$  成为  $G$  的子群。假定  $x, y \in H$ , 那末  $f(x) = f(y) = e'$ . 因为  $f$  是同态映射, 所以  $f(xy^{-1}) = f(x)(f(y))^{-1} = e' \cdot e'^{-1} = e'$ . 于是  $xy^{-1} \in H$ .

(ii)  $H$  成为  $G$  的正规子群。假定  $x \in H, z$  是  $G$  中任意元, 那末  $f(zxz^{-1}) = f(z)f(x)(f(z))^{-1} = f(z) \cdot e' (f(z))^{-1} = f(z)(f(z))^{-1} = e'$ . 所以  $zxz^{-1} \in H$ , 即  $zHz^{-1} \subset H$ . 由这即得  $H \subset z^{-1}Hz$ . 假如用  $z^{-1}$  代替  $z$ , 那末  $zHz^{-1} \supset H$ , 所以  $zHz^{-1} = H$ .

(iii)  $G' \cong G/H$ . 假定自  $G$  到  $G/H$  的自然映射是

$$\begin{array}{ccc} G & \xrightarrow{f} & G' \\ \phi \downarrow & \nearrow \psi & \\ G/H & & \end{array}$$

$\phi, x'$  是  $G'$  中任意元, 因为  $f$  是自  $G$  到  $G'$  上的同态映射, 所以在  $G$  中有适当的元  $x$  存在使  $f(x) = x'$ . 这样的  $x$  一般不是唯一确定的, 但是, 如果  $f(x) = f(x_1) = x'$ , 显

然  $f(xx_1^{-1}) = e'$ , 于是  $xx_1^{-1} \in H$ . 所以  $\phi(x) = \phi(x_1)$  由  $x'$  唯一确定。把这  $\phi(x)$  对应于  $x'$  的映射设为  $\psi$ , 那末  $\psi$  显然给出自  $G'$  到  $G/H$  的同构映射。 (証毕)

定理 3 中的  $H$ , 叫做同态映射  $f$  的核 (kernel), 写成  $\text{Ker } f$  (参照 44 页)。

**例 12** 对于可换群, 所有的子群是正规子群。譬如  $G = \mathbb{Z}$ , 如果  $H$  是  $\mathbb{Z}$  中用  $m \in \mathbb{Z} (m \neq 0)$  生成的子群 (它用  $m\mathbb{Z}$  表示), 那末  $G/H = \mathbb{Z}/m\mathbb{Z} = \mathbb{Z}_m$  (参照例 10)。

**例 13** 在  $G = \mathfrak{S}(\{1, 2, 3\})$  中,  $H = \{(1), (12)\}$  不是正规子群 (参照例 11)。 $\{(1), (123), (132)\}$  是正规子群, 而  $G/H$  成为阶为 2 的循环群。

**例 14** 指数是 2 的子群总是正规子群。特别, 交代群是对称群的正规子群。

[解] 假定  $H$  是  $G$  的指数是 2 的子群。如果  $x$  是  $G$  中不属于  $H$  的任意元, 因为  $Hx$  是关于  $\text{mod } H$  异于  $H$  的右剩余类, 所以  $G = H \cup Hx$ , 于是作为集合  $Hx = G - H$ . 根据完全同样的理由,  $xH$  也是  $G - H$ , 所以  $Hx = xH$ . 又假如  $x \in H$ , 因为  $H$  是子群, 所以  $xHx^{-1} = H$ . 于是  $H$  做成  $G$  的正规子群。

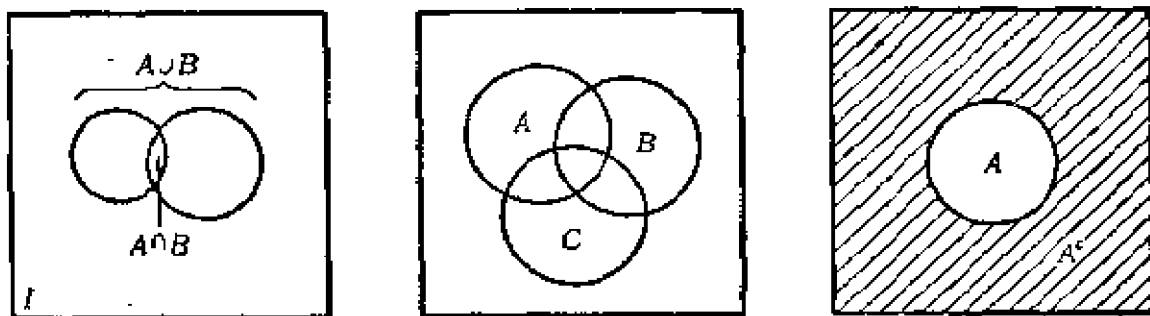
如前所述, 群所关連的各种事实出现于数学中各部门, 它們“表现”为何种形状完全根据計算的便利来处理。在最广意义下, 自

群  $G$  到  $G'$  的(到  $G'$  中的)同态映射,叫做  $G$  在  $G'$  的表现,但是希望  $G'$  是比  $G$  “具体的”并且  $G'$  的群算法是属于“便于计算”形式的。通常单说  $G$  群的表现时,是假定取  $GL(n, \mathbb{C})$  ( $n = 1, 2, \dots$ ) 作为  $G'$ ,  $GL(n, \mathbb{C})$  是复数体  $\mathbb{C}$  上  $n$  维向量空间  $V$  的自同构群,它们的元用  $n$  级正则矩阵表示。因为群算法用矩阵算法表示,所以在它的理论中当然能够引用第 1 章的诸结果。又在与群的联系中,上面的同态定理(定理 3)很重要。关于有限群的表现论将在第 3 章详述。

### § 23 Boole 代数

与 § 2 同样,对于一个集合  $I$  的子集  $A, B, C, \dots$ , 假如  $A, B$  的和集用  $A \cup B$  表示,  $A, B$  的交集用  $A \cap B$  表示, 那末下面各个法则显然成立:

- (i) 幂等律  $A \cup A = A, A \cap A = A.$
- (ii) 可换律  $A \cup B = B \cup A, A \cap B = B \cap A.$
- (iii) 结合律  $(A \cup B) \cup C = A \cup (B \cup C),$   
 $(A \cap B) \cap C = A \cap (B \cap C).$
- (iv) 吸收律  $A \cup (A \cap B) = A, A \cap (A \cup B) = A.$
- (v) 分配律  $(A \cup B) \cap C = (A \cap C) \cup (B \cap C),$   
 $(A \cap B) \cup C = (A \cup C) \cap (B \cup C).$



$$(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$$

图 23.1

关于  $I, \emptyset$ , 特别有

$$(vi) \quad I \cup A = I, \emptyset \cup A = A; I \cap A = A, \emptyset \cap A = \emptyset.$$

又假如  $A$  的(对于  $I$ )补集合  $I - A$  写成  $A^c$ , 那末

$$(vii) \quad A \cup A^c = I, A \cap A^c = \emptyset.$$

$$(viii) \quad \text{De Morgan 法则} \quad (A \cup B)^c = A^c \cap B^c, (A \cap B)^c = A^c \cup B^c.$$

$$(ix) \quad \text{对合律} \quad A^{cc} = A.$$

“Boole 代数”就是这种“集合族”的概念的一般化,它是作为下面这样的代数系而定义的。

**Boole 代数**  $L$  是元  $x, y, z, \dots$  的集合, 在  $L$  中任意两元  $x, y$  之间定义两种算法  $x \cup y, x \cap y$ , 这算法服从 (i) 幂等律, (ii) 可换律, (iii) 结合律, (iv) 吸收律, (v) 分配律诸法则。又  $L$  有两个特定的元  $1, 0$ , 使得

$$(vi) \quad 1 \cup x = 1, 0 \cup x = x; 1 \cap x = x, 0 \cap x = 0$$

成立。对于  $L$  的任意元  $x$ , 存在满足

$$(vii) \quad x \cup x^c = 1, x \cap x^c = 0$$

的  $x^c \in L$ .  $x \cup y$  叫做  $x, y$  的**结**,  $x \cap y$  叫做  $x, y$  的**交**。1, 0 分别叫做  $L$  的**单位元**, **零元**,  $x^c$  叫做  $x$  的**补元**。

以下,本节中  $L$  表示 Boole 代数。

**命题 1**  $x$  的补元唯一确定, 即如果  $x \cup y = 1, x \cap y = 0, x \cup z = 1, x \cap z = 0$ , 那末  $y = z$ .

$$\begin{aligned} \text{证明} \quad y &= 1 \cap y && (\text{由 vi}) \\ &= (x \cup z) \cap y = (x \cap y) \cup (z \cap y) && (\text{由 v}) \\ &= 0 \cup (z \cap y) = z \cap y = y \cap z, && (\text{由 vi, ii}) \end{aligned}$$

完全同样,  $z = y \cap z$ . 所以  $y = z$ .

**命题 2** 在  $L$ , (viii) De Morgan 法则  $(x \cup y)^c = x^c \cap y^c$ ,  $(x \cap y)^c = x^c \cup y^c$  及 (ix) 对合律  $(x^c)^c = x$  成立。

**証明** 命  $x^c \cap y^c = z$ , 假如能够証明  $x \cup y \cup z = 1, (x \cup y) \cap z = 0$ , 那末由命题 1,  $z = (x \cup y)^c$ . 但这时,  $x \cup y \cup z = x \cup y \cup (x^c \cap y^c) = x \cup ((y \cup x^c) \cap 1) = x \cup (y \cup x^c) = (x \cup x^c) \cup y = 1 \cup y = 1$ ,  $(x \cup y) \cap z = (x \cup y) \cap (x^c \cap y^c) = ((x \cup y) \cap x^c) \cap ((x \cup y) \cap y^c) = (0 \cup (y \cap x^c)) \cap ((x \cap y^c) \cup 0) = (y \cap x^c) \cap (x \cap y^c) = (x \cap x^c) \cap (y \cap y^c) = 0 \cap 0 = 0$ . 同样  $(x \cap y)^c = x^c \cup y^c$  也成立。

(ix) 由命题 1 自明。

**命题 3** 在  $L$ ,  $x \vdash x \cup y \Leftrightarrow y = x \cap y$ .

这时, 假如写成  $x \geq y$  (或  $y \leq x$ ), 那末

- (a)  $x \geq x$ ,
- (b)  $x \geq y, y \geq x \Rightarrow x = y$ ,
- (c)  $x \geq y, y \geq z \Rightarrow x \geq z$

成立。又  $x \cup y, x \cap y$  的特征如下:

- (d)  $x \cup y \geq x, x \cup y \geq y$ ,
- (e)  $z \geq x, z \geq y \Rightarrow z \geq x \cup y$ ,
- (d')  $x \cap y \leq x, x \cap y \leq y$ ,
- (e')  $z \leq x, z \leq y \Rightarrow z \leq x \cap y$ .

**証明** 假定  $x = x \cup y$ , 用吸收律,  $x \cap y = (x \cup y) \cap y = y$ . 反之同样成立。(a) ~ (e') 由下面諸式是显明的。

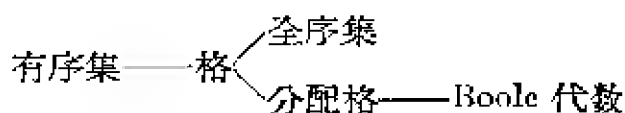
- (a)  $x \vdash x \cup x$  (由 i).
- (b)  $x = x \cup y = y \cup x = y$  (由 ii).
- (c)  $x = x \cup y = x \cup (y \cup z) = (x \cup y) \cup z = x \cup z$  (由 iii).
- (d)  $x \cup y = (x \cup x) \cup y = x \cup (x \cup y) = x \cup (y \cup x) = (x \cup y) \cup x$  (由 i, ii, iii),  $x \cup y \geq y$  也是同样。
- (e)  $z = z \cup y = (z \cup x) \cup y = z \cup (x \cup y)$  (由 iii).
- (d')  $x \cap y = (x \cap x) \cap y = x \cap (x \cap y)$  (由 i, iii),  $x \cap y \leq y$  也同样 (由 i, ii, iii).

(e')  $z = x \cap z = x \cap (y \cap z) = (x \cap y) \cap z$  (由 iii).

**系** 关于  $L$  中任意元  $x$ ,  $1 \geq x$ ,  $x \geq 0$ .

**注意 1** 命题 3 只用 Boole 代数公理中 i, ii, iii, iv 就能证明。只采用 Boole 代数公理中 i, ii, iii, iv 定义的代数系, 一般叫做格, 采用 i, ii, iii, iv, v 所得到的代数系, 叫做分配格。

在某集合  $S$  中两元  $x, y$  之间, 假定有用  $\leq$  表示的关系存在并且对于它, 命题 3 中的 (a), (b), (c) 又成立时, 那末  $S$  叫做由  $\leq$  给出顺序的有序集。在有序集  $S$  中, 假如两元  $x, y$  之间  $x \leq y$  或  $y \leq x$  必定有一成立时, 那末  $S$  叫做全序集。这些概念间广狭关系如下(左狭右广)



关于有序集与格的各自的理论, 在这里都没有机会深入。

**注意 2** 算法  $\cup, \cap$  叫做格算法, 依照这些算法结合的象  $((x \cup y) \cap z) \cup (x \cap y)$  这样的, 叫做“变数” $x, y, z$  的格多项式。在格多项式中把记号  $\cup, \cap$  互换又能够得到一个格多项式——在上例是  $((x \cap y) \cup z) \cap (x \cup y)$ ——它叫做对偶(dual)于原来格多项式的格多项式, 如此的变形叫做对偶变形。格和分配格的公理都能够用格多项式的等式来表示。对于这样等式的两边施行对偶变形, 也叫做对于这等式施行对偶变形, 所得到的等式是对偶于原来的等式。格和分配格的公理假如含一个等式, 也就必定含对偶于它的等式。根据这事实, 就说这公理是自己对偶的。于是假如自格和分配格的公理导出某个等式, 那末对偶于它的等式也必定能够导出。这事实叫做对偶原理。在 Boole 代数的公理中, 假如把  $\cup, \cap$  互换, 同时又把  $1, 0; x, x^c$  互换, 则在上述意义下成为“自己对偶”, 并且对偶原理成立。根据这原理在定理的证明中, 关于对偶的只要记述一方已足。

**例 1** 由  $I = \{1, 2\}$  的子集形成的 Boole 代数, 具有  $I, A = \{1\}, B = \{2\}, \emptyset$  四个元, 它的结, 交, 补元的表如后。

$\cup$	$\emptyset$	$A$	$B$	$I$	$\cap$	$\emptyset$	$A$	$B$	$I$	$X$	$\emptyset$	$A$	$B$	$I$
$\emptyset$	$\emptyset$	$A$	$B$	$I$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	$X^c$	$I$	$B$	$A$	$\emptyset$
$A$	$A$	$A$	$I$	$I$	$A$	$\emptyset$	$A$	$\emptyset$	$A$	$X^c$ 的表				
$B$	$B$	$I$	$B$	$I$	$B$	$\emptyset$	$\emptyset$	$B$	$B$					
$I$	$I$	$I$	$I$	$I$	$I$	$\emptyset$	$A$	$B$	$I$					
$X \cup Y$ 的表					$X \cap Y$ 的表									

一般,由  $I = \{1, 2, \dots, n\}$  的子集合形成的 Boole 代数  $B_n$  具有  $2^n$  个元, 它的  $\cup, \cap, ^c$  的表容易作出。具有有限个元的 Boole 代数与一个  $B_n$  同构。

**例 2** 假定  $L = \{P, Q, R, \dots\}$  是命题的集合, 解释  $P \cup Q$  为“ $P$  或  $Q$ ”,  $P \cap Q$  为“ $P$  并且  $Q$ ”,  $I$  为“真”,  $\emptyset$  为“伪”,  $P^c$  为“非  $P$ ”, 如果通常的论理学 (Aristoteles 的论理学) 成立, 那末“命题算”能够用 Boole 代数表示。譬如  $P \cup P^c = I$  意味着“ $P$  或非  $P$  中一个是真”。 $P \supseteq Q (\Leftrightarrow P = P \cup Q \Leftrightarrow Q = P \cap Q)$  解释为“假如  $P$  那末  $Q$ ” (在命题算中, 对于它, 象现在本文中使用的那样, 可以用  $P \Rightarrow Q$  的记法)。于是,  $P \supseteq Q, Q \supseteq R \Rightarrow P \supseteq R$  意味着三段论法 ( $P \Rightarrow Q, Q \Rightarrow R \Rightarrow (P \Rightarrow R)$ )。

Boole 代数是由 George Boole 在 19 世纪中叶作为“论理代数”而引入的 (The Mathematical Analysis of Logic, 1847; An Investigation into the Laws of Thought, 1854), 但现在它的理论已能够用到概率论和分析等诸方面 (测度论等), 在应用上计算机的理论等中也被引用。这些在这里都不能深入了, 下面只举简单应用的一例。

**例 3** 就收听无线电广播组  $A, B, C$  的情况进行调查, 得到这样的报告:  $n$  人中收听  $A$  组的  $a$  人, 收听  $B$  组的  $b$  人, 收听  $C$  组的  $c$  人, 收听  $A, B$  两方的  $d$  人, 收听  $B, C$  两方的  $e$  人, 收听  $C, A$  两方的  $f$  人, 今问收听  $A, B, C$  三方的有几人。

[解] 假定收听  $A, B, C$  各个组人的集合仍旧用  $A, B, C$  表示, 一般有限集合  $M$  中元的个数用  $|M|$  表示。关于个数, 显然

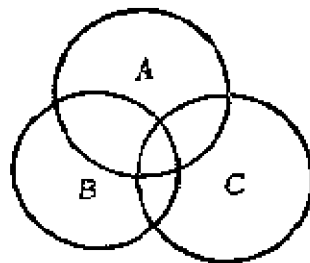


图 23.2

$$M = M_1 \cup M_2, M_1 \cap M_2 = \emptyset \Rightarrow |M| = |M_1| + |M_2|$$

成立。与 § 2 同样,  $M = M_1 \cup M_2, M_1 \cap M_2 = \emptyset$  ( $M$  是  $M_1$  与  $M_2$  的直和) 时,

写成  $M = M_1 + M_2$ , 那末

$$|M_1 + M_2| = |M_1| + |M_2|.$$

$M = M_1 \cup M_2$ , 但  $M = M_1 + M_2$  不成立时, 命  $M_1 \cap M_2 = M'_1$ ,  $M_2 \cap M'_1 = M'_2$ ,

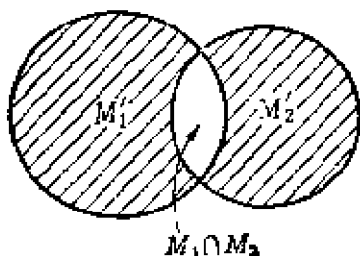


图 23.3

显然

$$M_1 = M'_1 + (M_1 \cap M_2), \quad M_2 = M'_2 + (M_1 \cap M_2),$$

$$M_1 \cup M_2 = M'_1 + M'_2 + (M_1 \cap M_2).$$

于是

$$\begin{aligned} |M_1 \cup M_2| &= |M'_1| + |M'_2| + |M_1 \cap M_2| \\ &= |M_1| + |M_2| - |M_1 \cap M_2|. \end{aligned}$$

由这公式得

$$\begin{aligned} |A \cup B \cup C| &= |A \cup B| + |C| - |(A \cup B) \cap C| \\ &= |A| + |B| - |A \cap B| + |C| - |(A \cap C) \cup (B \cap C)| \\ &= |A| + |B| + |C| - |A \cap B| \\ &\quad - (|A \cap C| + |B \cap C| - |A \cap B \cap C|) \\ &= |A| + |B| + |C| - |A \cap B| - |B \cap C| \\ &\quad - |C \cap A| + |A \cap B \cap C|. \end{aligned}$$

所以假如  $|A \cap B \cap C| = g$ , 那末

$$n = a + b + c - d - e - f + g.$$

由此式即能求得  $g$ .

## § 24 有 限 体

本节的目标是后面的定理 4 (162 页), 在它的证明中必须引用初等整数论及代数学中如下的一些事实 (i) ~ (ix)。

(i) **初等整数论的基本定理** 任意自然数  $n$  能够质因数分解为  $n = p_1^{e_1} \cdots p_r^{e_r}$  ( $p_i$  是质数,  $e_i \geq 0$ ).  $n'$  是又一自然数, 假如能够质因数分解为  $n' = p_1^{e'_1} \cdots p_r^{e'_r}$ , 那末  $e_i \geq e'_i$  ( $i = 1, \dots, r$ ) 时而且限于这时,  $n$  是  $n'$  的倍数 ( $n$  是  $n'$  的倍数,  $n'$  是  $n$  的约数, 用  $n' | n$  来表示)。

又对于上面的  $n, n'$ , 它的最大公约数  $(n, n')$  用  $p_1^{\min(e_1, e'_1)} \cdots p_r^{\min(e_r, e'_r)}$  ( $\min(e_i, e'_i)$  表  $e_i, e'_i$  中小的一数) 给出。  $n, n'$  的最小公倍数用  $p_1^{\max(e_1, e'_1)} \cdots p_r^{\max(e_r, e'_r)}$  ( $\max(e_i, e'_i)$  表  $e_i, e'_i$  中大的一数) 给出。

(ii) 假如  $(n, n') = 1$ , 这时  $n, n'$  叫做互质, 那末存在适合  $nx + n'x' = 1$  的  $x, x' \in \mathbb{Z}$ , 又其逆亦真。

(iii) 假定  $K$  是体,  $K$  上变数  $X$  的多项式, 即

$$f(X) = a_0 + a_1X + \cdots + a_kX^k, \quad a_i \in K, \quad i = 1, \dots, k \quad (24.1)$$

形状的式全体的集合成为  $K$  上代数 (§ 7), 叫做  $K$  上多项式环, 用  $K[X]$  表示。于 (24.1), 假如  $a_k \neq 0$ , 那末  $f(X)$  叫做  $k$  次多项式或  $f(X)$  的次数是  $k$ . 非 0 的“常数”  $a_0$  的次数是 0, 多项式 0 的次数不定义。假如  $k$  次多项式的集合用  $K^k[X]$  表示, 那末  $K[X] = \{0\} \div K^0[X] + K^1[X] + \cdots$  (作为集合的直和),  $\{0\} + K^0[X] + \cdots + K^k[X]$  用  $K_k[X]$  表示,  $K_k[X]$  中元, 叫做次数  $k$  以下的多项式。次数  $k$  以下的多项式能够写成 (24.1) 形状。 $K_k[X]$  形成  $K$  上  $k$  维向量空间,  $K[X]$  形成  $K$  上无限维向量空间。

(iv) 当  $f(X) \in K_k[X]$  时, 对于  $\alpha \in K$ , 假如  $f(\alpha) = 0$  即  $f(X) = 0$  在  $K$  中有根  $\alpha$ , 那就有适合  $f(X) = (X - \alpha)g(X)$  的  $g(X) \in K_{k-1}[X]$ . 假如  $\alpha_1, \dots, \alpha_\nu$  是  $f(X) = 0$  的  $\nu$  个不同的根, 那就有适合  $f(X) = (X - \alpha_1) \cdots (X - \alpha_\nu)h(X)$  这样的  $h(X) \in K_{k-\nu}[X]$  存在。于是“ $k$  次方程”  $f(X) = 0$  的根的个数不大于  $k$ .

(v) 关于  $K[X]$  中元, 有与上面关于自然数的 (i) 同样的事实成立:  $K[X]$  中元能够唯一地表为在  $K$  中“既约多项式”的积:  $f(X) = (p_1(X))^{e_1} \cdots (p_r(X))^{e_r}$ . 又两个多项式  $f_1(X), f_2(X)$  假如互质, 即假如它们的最大公约数  $(f_1(X), f_2(X))$  是 1, 那就有适合  $f_1(X)g_1(X) + f_2(X)g_2(X) = 1$  这样的  $K$  上多项式  $g_1(X), g_2(X)$ .

(vi) 假如  $L$  是含体  $K$  的体, 即  $K$  的扩张体, 那末  $L$  成为  $K$  上向量空间。特别,  $L$  是  $K$  上有限维向量空间时, 它的维数叫做  $L$  在  $K$  的维数, 用  $(L:K)$  表示。

(vii) 对于  $K[X]$  中元  $f(X)$ , 假如作  $K$  的适当扩张体  $L$ , 那末  $f(X)$  在  $L$  能够分解为一次因数, 即在  $L$ ,



$$f(X) = e(X - \alpha_1)^{\nu_1} \cdots (X - \alpha_r)^{\nu_r} \quad (\alpha_i \neq \alpha_j), \quad (24.2)$$

于是  $f(X) = 0$  的所有根  $\alpha_1, \dots, \alpha_r$  都在  $L$  中。这时  $L$  叫做  $f(X)$  的**分解体**。分解体中, 关于  $K$  的維数最小的, 叫做**最小分解体**。 $f(X)$  的最小分解体的維数不大于  $f(X)$  的次数。特别  $f(X)$  是既約时, 維数与次数一致。并且,  $f(X)$  的最小分解体除同构外是唯一确定的(即假如  $L, L'$  都是  $f(X)$  的最小分解体, 那末  $L, L'$  作为体是同构的)。

(viii) 对于  $K_k[X]$  中元  $f(X) = \sum_{i=0}^k a_i X^i$ ,  $K_{k-1}[X]$  中元  $f'(X) = \sum_{i=0}^{k-1} i a_i X^i$  叫做  $f(X)$  的**导函数**。映射  $f(X) \rightarrow f'(X)$  是自  $K$  上向量空間  $K_k[X]$  到  $K_{k-1}[X]$  的綫性映射。即对于  $a, b \in K, f, g \in K_k[X]$ ,

$$(af + bg)' = af' + bg'.$$

又关于积的导函数, 下面的公式成立:

$$(fg)' = f'g + fg'.$$

(ix) 在 (24.2) 中,  $\nu_i$  叫做  $f(X)$  的根  $\alpha_i$  的**重复度**。 $\nu_i = 1$  时,  $\alpha_i$  叫做  $f(X)$  的**单根**。 $f(X)$  只有单根的必要充分条件是  $f(X)$  与  $f'(X)$  互质。

上面除 (vii) 外想都是熟知的 ((ix) 用 (viii) 容易証明)。\* (vii) 在 § 14 也曾引用过。关于它的証明在后面例 4 的解中将有略示, 其詳可在同处引用的正田, 淺野的书籍中看到。

以上是預备知識的复习, 在进入本論的途中, 为了不走弯路, 首先証明下面关于可換群的两个引理。

**引理 1** 假定  $G$  是可換群。  $x, y \in G$ ,  $x, y$  的阶分別是  $m, n$ , 如果  $(m, n) = 1$ , 那末  $z = xy$  的阶是  $mn$ 。

**証明**  $z^{mn} = (xy)^{mn} = x^{mn} y^{mn} = (x^m)^n (y^n)^m = e$  (自第二边到第三边用  $G$  的可換性), 所以  $z$  的  $mn$  乘方無論如何是  $e$ 。于是  $z$  的阶是

$mn$  的約数。反之,  $z^l = e \Rightarrow mn | l$  可如下証明。假定  $z^l = x^l y^l = e$ , 那末  $e = (x^l y^l)^m = x^{ml} y^{ml} = y^{ml}$ , 于是  $n | ml$ , 但  $(m, n) = 1$ , 所以由 (ii) 有适合  $mh + nk = 1$  这样的  $h, k \in \mathbb{Z}$ . 因此  $l = mlh + nkl$  是  $n$  的倍数:  $n | l$ . 同样  $m | l$ . 因为  $(m, n) = 1$ , 所以  $mn | l$ .

**引理 2** 与前引理同样, 假定  $G$  是可換群,  $x, y \in G$ ,  $x, y$  的阶是  $m, n$ , 如果  $n \times m$  ( $n | m$  的否定), 那末  $G$  中有阶比  $m$  大的元  $z$ .

**証明**  $(m, n) = 1$  时, 由引理 1 是明显的。因此假定  $(m, n) > 1$ . 作  $m, n$  的质因数分解

$$m = p_1^{e_1} \cdots p_{r_1}^{e_{r_1}} p_{r_1+1}^{e_{r_1+1}} \cdots p_r^{e_r}, \quad n = p_1^{f_1} \cdots p_{r_1}^{f_{r_1}} p_{r_1+1}^{f_{r_1+1}} \cdots p_r^{f_r},$$

如果  $e_1 \geq f_1, \dots, e_{r_1} \geq f_{r_1}, e_{r_1+1} < f_{r_1+1}, \dots, e_r < f_r$ . 因为  $n \times m$ , 所以  $0 \leq r_1 < r$ . 于是命

$$m_1 = p_1^{e_1} \cdots p_{r_1}^{e_{r_1}}, \quad n_1 = p_{r_1+1}^{f_{r_1+1}} \cdots p_r^{f_r},$$

那末  $(m_1, n_1) = 1, m_1 | m, n_1 | n, m_1 n_1 > m$ . 命  $m = m_1 m'_1, n = n_1 n'_1, x^{m_1} = x_1, y^{n_1} = y_1$ , 显然  $x_1, y_1$  的阶是  $m_1, n_1$ . 由引理 1,  $z = x_1 y_1$  的阶  $m_1 n_1 > m$ .

**引理 3** 假定  $G$  是有限可換群, 对于任意自然数  $n$ ,  $G$  中满足  $x^n = e$  的元的个数如果不超过  $n$ , 那末  $G$  是循环群。

**証明** 設  $G$  的阶是  $g$ , 証明  $G$  中具有阶  $g$  的元即可。今命  $x_1$  是  $G$  中任意元,  $x_1$  的阶是  $m_1$ , 假如  $m_1 = g$  那就好了。如果  $m_1 < g$ , 因为  $G - \{e, x_1, x_1^2, \dots, x_1^{m_1-1}\} = M_1 \neq \emptyset$ , 所以能够自  $M_1$  取一个元  $y_1$ . 假定  $y_1$  的阶是  $n_1$ , 那末  $n_1 \times m_1$ . 这是因为, 如果  $n_1 | m_1, m_1 = n_1 m'_1$ , 那末  $y_1^{m_1} = (y_1^{n_1})^{m'_1} = e$ . 于是  $G$  中  $(m+1)$  个元  $e, x_1, \dots, x_1^{m_1-1}, y_1$  都满足  $x^{m_1} = e$ . 这与假設矛盾。所以由引理 2,  $G$  中具有阶比  $m_1$  大的元  $x_2$ . 假如  $x_2$  的阶  $m_2 = g$ , 那就好了。如果  $m_2 < g$ , 与上面同样进行能够得到阶比  $m_2$  大的元  $x_3$ . 因为数列  $m_1 < m_2 < \dots$  在有限項 (最多也不过  $g$  項) 后达到  $m_k = g$ , 于是引理得証。

以上都是准备, 现在进入本题。

在 § 22 例 10, 看到关于自然数  $m$ , 把  $\mathbb{Z}$  中元关于  $\text{mod } m$  的剩余类形成的群定义为  $\mathbb{Z}_m$ ,  $\mathbb{Z}_m$  成为(关于加法)阶  $m$  的循环群。在  $\mathbb{Z}_m$  中元之間再如下定义乘法。即假如  $x \equiv x' \pmod{m}$ ,  $y \equiv y' \pmod{m}$ , 因为  $xy \equiv x'y' \pmod{m}$ , 所以根据  $(x)_m(y)_m = (xy)_m$ , 可定义  $\mathbb{Z}_m$  中元  $(x_m), (y_m)$  之間的乘法。这时  $\mathbb{Z}_m$  显然成为可换环 (§ 7), 但一般不一定成为体。在体  $K$  中对于异于 0 的元, 因为它有关于乘法的逆元, 所以  $a, b \in K, ab=0 \Rightarrow a=0$  或  $b=0$ 。这是因为如果  $ab=0, a \neq 0$ , 那末  $0 = a^{-1}0 = a^{-1}(ab) = 1 \cdot b = b$ 。于是当  $m = m_1 m_2 (m_1, m_2 > 1)$  时,  $(m_1)_m, (m_2)_m$  都不是  $(0)_m$ , 但  $(m_1)_m \cdot (m_2)_m = (m_1 m_2)_m = (0)_m$ , 所以  $\mathbb{Z}_m$  不得为体。可是下面的基本命题成立。

**命题 1** 假如  $p$  是质数, 那末  $\mathbb{Z}_p$  是体。

**証明**  $(x)_p \neq (0)_p$  即  $x \not\equiv 0 \pmod{p}$  时証明存在适合  $(x)_p(y)_p = (1)_p$ , 即  $xy \equiv 1 \pmod{p}$  的  $y$  即可。因为  $x \not\equiv 0 \pmod{p}$ , 所以  $(x, p) = 1$ 。于是由上述(ii)适合  $xy + pz = 1$  的  $y, z \in \mathbb{Z}$  存在。这就意味着  $xy \equiv 1 \pmod{p}$ 。 (証毕)

象  $\mathbb{Z}_p$  这样, 具有有限个元的体, 叫做有限体。

**例 1** 假定  $p=2$ , 那末  $\mathbb{Z}_p = \{(0), (1)\}$ , 它的元之間的加法, 乘法給出如下:

$$\begin{aligned} (0) + (0) &= (0), & (0) + (1) &= (1) + (0) = (1), & (1) + (1) &= (0), \\ (0)(0) &= (0), & (0)(1) &= (1)(0) = (0), & (1)(1) &= (1). \end{aligned}$$

**命题 2** 任意有限体  $K$  是对于某质数  $p$  的  $\mathbb{Z}_p$  (与它同构的体) 的扩张体。

**証明** 假定  $K$  中用它的乘法单位元 1 生成的加法群的子群是  $K_0 = \{0, 1, 1+1, \dots\}$ , 如果  $K_0$  的阶(即 1 在  $K$  的加法群中的阶)是  $m$ , 那末

$$\begin{aligned} 1 + 1 + \dots + 1 &= 0, \\ \leftarrow m \text{ 个 } \rightarrow \end{aligned}$$

如果  $m$  不是质数,  $m = m_1 m_2$  ( $m_1, m_2 > 1$ ), 那末在  $K$  中由分配律显然

$$\underbrace{(1 + \cdots + 1)}_{\leftarrow m_1 \text{ 个} \rightarrow} \underbrace{(1 + \cdots + 1)}_{\leftarrow m_2 \text{ 个} \rightarrow} = \underbrace{1 + \cdots + 1}_{\leftarrow m \text{ 个} \rightarrow} = 0.$$

于是由在命题 1 上面的注意,  $1 + \cdots + 1 = 0$  或  $1 + \cdots + 1 = 0$ , 这与  $m$  是 1 的阶的假定矛盾。所以  $m$  不得不是质数  $p$ , 这样就得  $K_0 \cong \mathbb{Z}_p \subset K$ . (証毕)

象在上面証明中看到的一样, 对于任意体  $K$  (不是有限体也可), 在加法群中 1 的阶是质数  $p$  或是无限。当它的阶是  $p$  时,  $K$  的特征数叫做  $p$ , 是无限时  $K$  的特征数叫做 0。特征数  $p$  的体都是  $\mathbb{Z}_p$  (与它同构的体) 的扩张体。同样, 特征数 0 的体是有理数体 (与它同构的体) 的扩张体。因此  $\mathbb{Z}_p$  叫做特征数  $p$  的质体, 有理数体叫做特征数 0 的质体。

**命题 3** 特征数  $p$  的有限体  $K$  中元的个数等于  $p$  的某乘幂  $p^n$ .

**証明**  $K$  是  $\mathbb{Z}_p$  的扩张体, 維数  $(K : \mathbb{Z}_p) = n$  当然是有限。把  $K$  看成  $\mathbb{Z}_p$  上向量空間时, 它的基底如果是  $e_1, \cdots, e_n$ , 那末  $K$  的任意元  $x$  能够唯一的表为

$$x = \alpha_1 e_1 + \cdots + \alpha_n e_n, \quad \alpha_i \in \mathbb{Z}_p$$

的形状。因为各个  $\alpha_i$  能够各自独立地取  $\mathbb{Z}_p$  中  $p$  个元, 所以  $x$  的个数是  $p^n$ .

**命题 4** 自  $(K : \mathbb{Z}_p) = n$  的有限体  $K$  只除去 0 的集合  $K^* = K - \{0\}$  关于乘法所成的群是阶为  $p^n - 1$  的循环群。

**証明**  $K^*$  的阶显然是  $p^n - 1$ , 又根据在上面引用的 (iv), 关于任意自然数  $m$  满足  $x^m = 1$  的  $K$  中元的个数不超过  $m$ , 所以由引理 3,  $K^*$  成为循环群。

**系**  $K$  中所有元都满足方程  $x^{p^n} = x$ .

**例 2** 假定  $x \in \mathbb{Z}$ ,  $p$  是任意质数, 那末  $x^p \equiv x \pmod{p}$  (Fermat 定理)。

[解] 因为体  $Z_p$  中元的个数是  $p$ , 所以对于其中元  $(x)$ , 由上系  $(x)^p = (x)$  成立。于是  $(x^p) = (x)$ , 此即意味着  $x^p \equiv x \pmod{p}$ 。

例 3  $Z_7^*$  能够用  $(-2)$  生成。

[解] 因为  $Z_7^*$  的阶是 6, 所以其元的阶是 1, 2, 3 中之一。但是  $(-2) \neq (1)$ ,  $(-2)^2 = (4) \neq (1)$ ,  $(-2)^3 = (-8) = (5) \neq (1)$ , 所以  $(-2)$  的阶是 6, 因此  $Z_7^*$  能够用  $(-2)$  生成。

**定理 4** 对于质数  $p$  与任意自然数  $n$ , 存在具有  $p^n$  个元的有限体, 它除同构外是唯一确定的。

**证明** 假定  $Z_p$  中  $p^n$  次多项式  $X^{p^n} - X - f(X)$  的最小分解体是  $K$ 。因为  $f(X)$  的导函数  $f'(X) = -1$ , 所以最大公约数  $(f(X), f'(X)) = 1$ , 因此  $f(X)$  在  $K$  中有  $p^n$  个单根。命  $p^n = q$ , 假定它们的根是  $\alpha_1, \alpha_2, \dots, \alpha_q$  来证明  $K$  正好只由这  $q$  个元形成。实际上, 假如  $f(\alpha) = 0, f(\beta) = 0$  即  $\alpha^q = \alpha, \beta^q = \beta$ , 那末  $K$  的特征数是  $p$ , 因而  $K$  中任意元的  $p$  倍是 0, 又二项系数  $\binom{q}{k} = \binom{p^n}{k}$  对于  $1 \leq k \leq q-1$  是  $p$  的倍数)

$$(\alpha \pm \beta)^q = \alpha \pm \beta, \quad (\alpha\beta)^q = \alpha\beta.$$

$$\text{如果 } \alpha \neq 0, \quad \left(\frac{\beta}{\alpha}\right)^q = \frac{\beta}{\alpha}.$$

即只由  $f(X) = 0$  的根已能成为体。因为  $K$  是“最小”分解体, 所以  $K = \{\alpha_1, \dots, \alpha_q\}$ , 又由命题 4 的系与最小分解体的唯一性, 具有  $p^n$  个元的有限体只有这个  $K$  (与它同构的体)。(证毕)

上面具有  $q = p^n$  个元的有限体  $K$  是 Galois 导入的, Dickson 因此常常写成  $GF(q)$  ( $GF$  是 Galois Field 的略)。以上已表明  $GF(q)$  唯一存在。如命题 3 所示,  $GF(q)$  的加法群是  $n$  个  $Z_p$  的加法群的直和, 如命题 4 所示, 乘法群  $(GF(q))^*$  是阶为  $q-1$  的循环群。 $GF(q)$  与代数整数论也深有联系。又考虑  $GL(n, GF(q))$  及它的子群能够得到有限群的很饶趣的实例。在应用上能够利用

实验设计法。

关于  $GF(q)$  的基本事项, 理论的尽述于上, 但利用实验设计法等时, 实际上引起了作  $GF(q)$  中元之间加法, 乘法表的必要。这无非是把  $f(X) = 0$  在  $\mathbb{Z}_p$  中来“解”。以下示其一例。

例 4 求作  $GF(3^2)$  的加法, 乘法表。

[解]  $K = GF(3^2)$  是  $\mathbb{Z}_3 = \{0, 1, 2\}$  (为了以下简单, 关于 mod 3 的剩余类(0), (1), (2)用 0, 1, 2 表示) 的二次扩张。 $f(X) = X^2 - X = X(X^2 - 1)$  应该有二次既约因式  $g(X)$ ,  $K$  能够“添加”  $g(X) = 0$  的根于  $\mathbb{Z}_3$  得出  $(f(X))$  的二次既约因式如果有几个, 因为把它的任一个作为  $g(X)$  也能够得到同构的  $K$ , 所以不论那一个作为  $g(X)$  都可以。因为  $X^2 - 1 = (X^2 + 1)(X^2 - 1) = (X^2 + 1)(X^2 + 1)(X^2 - 1)$ ,  $X^2 + 1$  对于 mod 3 是既约(实际上  $0^2 + 1 = 1, 1^2 + 1 = 2, 2^2 + 1 = 2$ , 即使  $X = 0, 1, 2$  中任一个  $X^2 + 1$  也不是 0)。所以“添加”  $X^2 + 1$  的根于  $\mathbb{Z}_3$  就能够得到  $K$ 。

于是 Galois 象下面这样来考虑。例如复数体  $\mathbb{C}$  能够“添加”  $\sqrt{-1}$  于  $\mathbb{R}$  得出, 但是, 如果代数的考虑, 于  $\mathbb{R}$  添加  $\sqrt{-1}$  不外是把  $\mathbb{R}[X]$  用 mod  $(X^2 + 1)$  来计算(把  $\sqrt{-1}$  象“变数”来考虑,  $(\sqrt{-1})^2 + 1$  出现时假定为 0)。同样, 不论何体, 譬如现今的例  $\mathbb{Z}_3$ , 所谓于它“添加”  $X^2 + 1$  的根, 就是把  $\mathbb{Z}_3[X]$  用 mod  $(X^2 + 1)$  来计算——实际上, 象它那样做能够得到  $\mathbb{Z}_3$  的扩张体, 此可与  $\mathbb{Z}_p$  是体同样证明。 $\mathbb{Z}_3[X]$  用 mod  $(X^2 + 1)$  来计算时,  $X$  的类暂时用  $i$  表示(象这样所得到的  $\mathbb{Z}_p$  的扩张体中元有时叫做 Galois 的虚数)。因此  $i^2 = -1$ , 我们的  $K$  中元能够写成  $a + bi$ ,  $a, b \in \mathbb{Z}_3$  的形状。于是  $K^*$  的阶是 8, 能够找到阶 8 的元即可。写出  $i$  的幂来看,  $1, i, i^2 = -1, i^3 = -i, i^4 = 1$ , 所以  $i$  的阶是 4。不在其中  $K^*$  中的元, 如引理 3 的证明中所示, 应该有自乘 4 次而不是 1 的元。假如自乘 4 次不成为 1, 那末它的阶不得不是 8。例如  $1 + i$  就是这样的。实际上,

$$\begin{aligned}(1+i)^2 &= -i, & (1+i)^3 &= -i(1+i) = 1-i, \\(1+i)^4 &= -1, & (1+i)^5 &= -1-i, & (1+i)^6 &= i, \\(1+i)^7 &= -1+i, & (1+i)^8 &= 1.\end{aligned}$$

实行  $GF(3^2)$  的计算时, 利用右边那样的图式颇为便利。

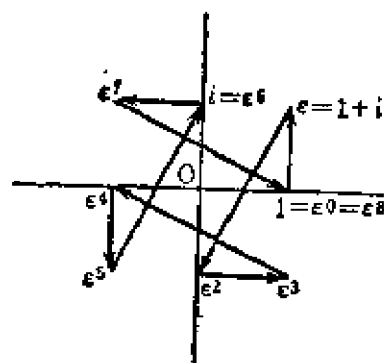


图 24.1

### 第3章 有限群的表现論

#### § 25 表現空間与不变子空間, 可約表現与既約表現

因为在这章所討論的向量空間都假定是有限維的, 而且是在复数域  $C$  上, 所以今后不再一一声明。于是  $n$  維向量空間  $V$  的自同构映射全体所形成的群  $GL(V)$  就与  $GL(n, C)$  同构。

如在第2章 § 22 所述, 所謂群  $G$  的表現指的是自  $G$  到  $GL(n, C)$  的同态映射 (特別, 当它是同构映射时, 就叫它做同构表現或忠实表現), 而自然数  $n$  叫做这个表現的次数。假如  $\dim V = n$ , 因为  $GL(V) \cong GL(n, C)$ , 所以  $G$  的表現  $\rho$  又可以看成是自  $G$  到  $GL(V)$  的同态映射。如果自  $G$  到  $GL(V)$  的同态映射  $\rho$  給定时,  $V$  叫做  $G$  的表現  $\rho$  的表現空間 (或者叫  $\rho$  做在  $V$  的表現)。于是, 表現的次数就是表現空間的維数。表現空間的討論有助于把群表現論作几何学地描述。

假定  $\rho$  是群  $G$  在  $V$  的表現, 那末对于  $a, b \in G$  有  $\rho(a), \rho(b), \rho(ab^{-1}) \in GL(V)$ , 并且

$$\rho(a)(\rho(b))^{-1} = \rho(ab^{-1}).$$

**例 1** 假設  $G$  是任意群,  $V$  是任意向量空間, 那末对于  $G$  的所有元使与  $e_V$  ( $V$  的恒等映射) 对应, 就給出  $G$  的一个表現。这是“自明的表現”。但在討論  $G$  的表現全体时, 不可忽視。它称为  $G$  在  $V$  的恒等表現。(如果  $G$  不是单位群, 恒等表現就不是同构表現。)

**例 2** 假設  $V$  是任意向量空間,  $\{e_V, -e_V\}$  ( $-e_V$  是对于  $x \in V$  使  $-x \in V$  对应的映射) 构成  $GL(V)$  中阶是 2 的子群。再假設  $G$  具有指数是 2 的子群 (因而是  $G$  的正規子群)  $H$  时, 令  $G = H \cdot Ha$ , 那末对于  $H$  的元使  $e_V$  对应, 对于  $Ha$  的元使  $-e_V$  对应的映射就給出  $G$  在  $V$  的表現, 它叫做  $G$  (在  $V$ ) 的交代表現。

**例 3** 假如  $G \subset GL(n, C)$ , 对于  $G$  的各元使它自身对应的映射当然给出  $G$  的同构表現。它叫做  $G (\subset GL(n, C))$  的**自然表現**。

当  $\rho_1, \rho_2$  是  $G$  分别在  $V_1, V_2$  的表現时, 假如有自  $V_1$  到  $V_2$  的同构映射  $f$ , 并且对于  $G$  中任意元  $a$ ,

$$f \circ \rho_1(a) = \rho_2(a) \circ f \text{ ①,}$$

那末  $\rho_1, \rho_2$  叫做**等价的或相似的表現**, 写成  $\rho_1 \sim \rho_2$ 。显然, 等价表現具有相同的次数, 这关系  $\sim$  滿足反射、对称、推移三律。这时表現空間  $V_1, V_2$  也叫做**等价的或同构的**(参照 174 頁)。

$$\begin{array}{ccc} V_1 & \xrightarrow{\rho_1(a)} & V_1 \\ f \downarrow & & \downarrow f \\ V_2 & \xrightarrow{\rho_2(a)} & V_2 \end{array}$$

特別, 如果  $\dim V = n$ , 在  $V$  取基底  $(a_1, \dots, a_n)$ , 那末  $V$  的坐标系  $\varphi = \varphi(a_1, \dots, a_n)$  就确定了, 由  $\varphi, V$  能够同构映射于  $C^n$ 。因之,  $G$  的表現  $\rho$  与  $G$  在  $C^n$  的表現  $a \rightarrow P(a) = \varphi \circ \rho(a) \circ \varphi^{-1}$  成为等价。 $P(a)$  是  $n$  級正則矩陣。 $a \rightarrow P(a)$  叫做  $G$  的  $n$  級**矩陣表現**。也叫它为  $\rho$  关于  $V$  的坐标系  $\varphi$  的矩陣表現。假如把  $V$  的坐标自  $\varphi$  变换到  $\psi$ , “坐标变换的矩陣”如果是  $\psi \circ \varphi^{-1} = T$  时, 就得到矩陣表現  $a \rightarrow TP(a)T^{-1}$ , 它叫做与  $a \rightarrow P(a)$  等价的, 或相似的矩陣表現。

假如給定了  $G$  在  $V$  的表現  $\rho$ , 那末

$$\rho(G) = \{\rho(a); a \in G\}$$

是  $GL(V)$  的子集合, 对于  $\rho(G)$  的任意元  $\rho(a)$ , 使

$$\rho(a)(W) \subset W$$

这样的  $V$  的子空間  $W$ , 叫做  $\rho$  的**不变子空間**。假如  $\rho$  的不变子空間全体的集合是  $\Sigma(\rho)$ , 显然  $\Sigma(\rho) \ni \{0\}, V$ 。又与第 1 章 § 4

① 也就是对于  $V_1$  中任意向量  $V_1$  及  $G$  中任意元  $a$  等式  $f[\rho_1(a)V_1] = \rho_2(a) \circ fV_1$  成立。——譯者注



中命题 1, 2 完全一样能够得到下面的命题。

**命题 1**  $\mathfrak{B}(\rho) \ni W_\alpha \Rightarrow \bigcap_\alpha W_\alpha \in \mathfrak{B}(\rho)$ .

**命题 2** 假如  $M$  是  $V$  的任意子集合, 那末  $\mathfrak{B}(\rho)$  中存在唯一含  $M$  的“最小”元  $W(M)$ .  $W(M)$  叫做由  $M$  生成的  $\rho$  的不变子空间。特别, 如果  $M = \{x\}$ , 那末

$$W(\{x\}) = \left\{ \sum_{a \in G} \lambda_a \rho(a)x; \lambda_a \in \mathbb{C}, (\lambda_a \text{ 除有限个外都是 } 0) \right\}.$$

**定理 1** 假设  $\rho$  是群  $G$  在  $n$  维向量空间  $V$  的表现,  $\rho$  具有  $\{0\}$ ,  $V$  以外的不变子空间  $W$ . 这时, 在  $V$  中如果取适当的坐标系  $\varphi$ , 那就能得到由下面那样形状的  $G$  的矩阵表现。

$$a \rightarrow P(a) = \begin{pmatrix} A(a) & B(a) \\ O_{n_2, n_1} & C(a) \end{pmatrix} \begin{matrix} \uparrow n_1 \\ \downarrow \\ \uparrow n_2 \\ \downarrow \end{matrix}, \quad n_1 = \dim W, \\ \leftarrow n_1 \rightarrow \leftarrow n_2 \rightarrow$$

又它的逆也成立。

**证明** 因为  $W \neq \{0\}$ ,  $V$ , 所以  $0 < \dim W = n_1 < n$ . 命  $n_1 + n_2 = n$ , 那末  $0 < n_2 < n$ . 令  $(a_1, \dots, a_{n_1})$  为  $W$  的基底, 因为  $V$  的基底能够取  $(a_1, \dots, a_{n_1}, a_{n_1+1}, \dots, a_n)$  的形状 (§5, 定理 5, 系 4)。于是命  $P(a) = (\alpha_{ij})$  时, 由 §8 就有

$$P(a) \cdot a_j = \sum_{i=1}^n \alpha_{ij} a_i,$$

但  $\rho(a)W \subset W$ , 所以当  $j = 1, \dots, n_1$  时, 有  $\alpha_{ij} = 0, i = n_1 + 1, \dots, n$ . 因此  $P(a)$  就成为上面形状的矩阵。

反之, 假如有象上面那样形状的矩阵表现, 如果在给出这表现的  $V$  的基底中, 由最初  $n_1$  个向量生成的子空间是  $W$ , 那末  $W$  显然是  $\rho$  的不变子空间。

**系** 假如群  $G$  的表现  $\rho$  的表现空间  $V$  能够表为不变子空间

$W_1, \dots, W_k$  的直和, 即

$$V = W_1 \oplus \dots \oplus W_k, \quad W_i \in \mathfrak{S}(\rho),$$

那末在  $V$  如果取适当的坐标系, 就能够得到  $G$  象下面形状的矩阵表现

$$a \rightarrow P(a) = Q_1(a) \oplus \dots \oplus Q_k(a).$$

这里,  $Q_i(a)$  的级数等于  $\dim W_i$ , 而  $a \rightarrow Q_i(a)$  成为  $G$  在  $W_i$  的表现  $\kappa_i$ . (系毕)

这时, 表现  $\rho$  叫做  $\kappa_1, \dots, \kappa_k$  的直和, 可如下写出

$$\rho = \kappa_1 \oplus \dots \oplus \kappa_k.$$

群  $G$  的表现  $\rho$  的表现空间  $V$  具有异于  $\{0\}$  及  $V$  的不变子空间时——即  $G$  具有在定理 1 中所说的那样形状的矩阵表现时——表现  $\rho$  叫做可约的, 不是可约的表现, 叫做既约的。  $\rho$  是可约, 且它的表现空间  $V$  成为两个以上 (不是  $\{0\}$ ) 不变子空间的直和时——即由定理 1 系,  $\rho$  成为几个表现的直和时—— $\rho$  就叫做直可约。

**例 4** 1 级表现都是既约的。

**例 5** 对于  $G$  的表现  $\rho$  的表现空间  $V$  的任意两个 1 维子空间  $V_1, V_2$ , 假如存在满足  $\rho(a)V_1 = V_2$  这样的  $a \in G$ , 那末  $\rho$  是既约的。

[解] 假设  $W$  是  $\rho$  异于  $\{0\}$  的不变子空间, 如果  $W \ni a \neq 0$ , 由命题 2 与我们的假设, 就得到  $W = V$ 。

**例 6**  $GL(n, C), U(n, C)$  的自然表现都是既约的。

[解] 由例 5 容易明白。

## § 26 Schur 引理

有限群的表现论在前世纪末由 Frobenius 创始, 而且大体上完成了, 1920 年 I. Schur 给以显著的简化。成为他方法的基础的是所谓“Schur 引理”这个简单命题。它不但是在群表现论中, 而且还是应用很广的有用命题。Schur 把这命题作为矩阵运算的一个定理给出。于此, 我们用下面与它稍异的形式来表达。

在前节,曾經定义群  $G$  的表現  $\rho$  的不變子空間,既約性、可約性等,現在把这些概念稍予擴張。一般,假定向量空間  $V$  的自同構群  $GL(V)$  的任意子集合叫做  $\mathfrak{A}(V)$  集合。如果  $A$  是一个  $\mathfrak{A}(V)$  集合,  $A$  中各元  $\rho_\alpha$  是自  $V$  到  $V$  的正則綫性映射,假如  $V$  的子空間  $W$  对于任意  $\rho_\alpha \in A$  常常有  $\rho_\alpha(W) \subset W$ , 那末  $W$  叫做  $A$  的不變子空間(在前节討論的是  $A = \{\rho(a); a \in G\} = \rho(G)$  的情况。 $\rho(G)$  是与  $G$  同态的群,但一般沒有必要要求  $\mathfrak{A}(V)$  集合成为群)。关于  $A$  的不變子空間  $\mathfrak{B}(A)$ , 与前节命题 1, 2 及定理 1 完全同样的命题显然都是成立的。当  $\mathfrak{B}(A) = \{\{0\}, V\}$  时,  $A$  叫做是既約的。

假定  $V_1, V_2$  是两个綫性空間,  $A_1, A_2$  分別是  $\mathfrak{A}(V_1)$  集合及  $\mathfrak{A}(V_2)$  集合,  $A_1, A_2$  中元一般用  $\rho_\alpha^{(1)}, \rho_\beta^{(2)}$  表示。自  $V_1$  到  $V_2$  的綫性映射  $f$  如果滿足下面两条件  $(S_1), (S_2)$ , 那末  $f$  叫做自  $A_1$  到  $A_2$  的协变变换。

$$\begin{array}{ccc}
 V_1 & \xrightarrow{\rho_\alpha^{(1)}} & V_1 \\
 f \downarrow & & \downarrow f \\
 V_2 & \xrightarrow{\rho_\beta^{(2)}} & V_2
 \end{array}
 \quad (S_1) \quad \text{对于任意 } \rho_\alpha^{(1)} \in A_1, \text{ 存在使}$$

$$f \circ \rho_\alpha^{(1)} = \rho_\beta^{(2)} \circ f \quad (25.1)$$

成立的  $\rho_\beta^{(2)} \in A_2$ .

$(S_2)$  对于任意  $\rho_\beta^{(2)} \in A_2$ , 存在使 (25.1) 成立的  $\rho_\alpha^{(1)} \in A_1$ .

**定理 2** (Schur 引理) 假定  $V_1, V_2$  是两个綫性空間,  $A_1, A_2$  分別是既約的  $\mathfrak{A}(V_1)$  集合和既約的  $\mathfrak{A}(V_2)$  集合, 如果  $f$  是自  $A_1$  到  $A_2$  的协变变换, 那末 (i)  $f=0$ , 或 (ii)  $f$  是同构映射, 两者必居其一。

**証明**  $\text{Im } f = V'_2$  是  $V_2$  的子空間, 并且能够証明  $V'_2 \in \mathfrak{B}(A_2)$ . 实际上, 假如  $y \in V'_2$  即  $y = f(x)$ ,  $x \in V_1$ , 那末由  $(S_2)$ , 对于任意  $\rho_\beta^{(2)} \in A_2$ , 有滿足  $\rho_\beta^{(2)}(y) = \rho_\beta^{(2)} \circ f(x) = f \circ \rho_\alpha^{(1)}(x)$  的  $\rho_\alpha^{(1)} \in A_1$ . 因为  $A_1$  是  $\mathfrak{A}(V_1)$  集合, 当然  $\rho_\alpha^{(1)}(x) \in V_1$ , 因此  $\rho_\beta^{(2)}(y) \in \text{Im } f = V'_2$ . 与这完全同样, 能够証明  $\text{Ker } f = V'_1 \in \mathfrak{B}(A_1)$ .

由  $A_1, A_2$  既約性的假定, 得  $V'_1 = \{0\}$  或  $V_1$ ,  $V'_2 = \{0\}$  或  $V_2$ ,

如果  $V'_1 = V_1$ , 当然  $V'_2 = \{0\}$ , 因此  $f = 0$ . 不论怎样, 如果  $V'_2 = \{0\}$ , 那末  $f = 0$ . 所以就有 (i) 的情况。否则,  $V'_1 = \{0\}$ ,  $V'_2 = V_2$ , 即  $f$  是全单射, 因此不得不是同构映射。所以有 (ii) 的情况。

**系** 假定  $\rho_1, \rho_2$  是群  $G$  分别在  $V_1, V_2$  的既约表现, 如果对于任意  $a \in G$ , 存在满足

$$\rho_2(a) \circ f = f \circ \rho_1(a)$$

的  $f \in L(V_1, V_2)$ , 那末  $f = 0$  或  $\rho_1 \sim \rho_2$ . (系毕)

为了叙述下面定理, 对于  $\mathfrak{U}(V)$  集合  $A$ , 定义  $\{\sigma; \sigma \in \mathfrak{S}(V), \rho \circ \sigma = \sigma \circ \rho, \forall \rho \in A\}$  为  $A$  的**交换子集合**  $A'$ .  $A'$  中元——即  $\mathfrak{S}(V)$  中与  $A$  中所有元可交换的元——叫做  $A$  的**交换子**。

**命题 3** 假如  $A$  是任意  $\mathfrak{U}(V)$  集合, 那末  $A' \cup \{0\} = \mathfrak{U}'$  是  $C$  上的可除代数(参照第 1 章 §7, 例 14)。

**证明** 因为  $A' \subset \mathfrak{S}(V)$ , 所以在  $A'$  中元  $\sigma, \sigma_1, \sigma_2$  及  $\lambda \in C$  之间, 能够定义乘法  $\sigma_1 \circ \sigma_2$  (作为映射的褶合), 加法  $\sigma_1 + \sigma_2$  及  $\lambda \sigma$  (作为  $\mathfrak{S}(V)$  中元, 依 §7 的意义)。由交换子的定义, 显然

$$\sigma, \sigma_1, \sigma_2 \in A' \Rightarrow \sigma_1 \circ \sigma_2, \sigma_1 + \sigma_2, \lambda \sigma \in A'.$$

又  $\lambda(\sigma_1 \circ \sigma_2) = \lambda \sigma_1 \circ \sigma_2 = \sigma_1 \circ (\lambda \sigma_2)$

也是显然的。于是  $A'$  是  $\mathfrak{S}(V)$  的子环, 并且成为  $C$  上的代数。但由定理 2, 假如  $\sigma \in A'$  不是 0, 那末  $\sigma \in GL(V)$ , 因此  $\sigma^{-1} \in GL(V)$ , 于是由交换子的定义, 显然  $\sigma^{-1} \in A'$ . 所以  $A'$  是  $C$  上的可除代数。

**定理 3** 假定  $V$  是有限维,  $A$  是既约的  $\mathfrak{U}(V)$  集合, 那末  $A'$  是与  $C$  同构的体。

**证明** 假定  $\sigma$  是  $A'$  中任意元, 如果  $\sigma$  的特征值之一是  $\alpha$ , 因为  $\text{Ker}(\sigma - \alpha) \neq 0$ , 那末  $\sigma - \alpha$  不是同构映射。但是对于既约  $A$  中任

意元  $\rho$ , 因为  $(\sigma - \alpha) \circ \rho = \rho \circ (\sigma - \alpha)$  成立, 所以由定理 2 系, 不得

$$\begin{array}{ccc} V & \xrightarrow{\rho} & V \\ \sigma - \alpha \downarrow & & \downarrow \sigma - \alpha \\ V & \xrightarrow{\rho} & V \end{array}$$

不  $\sigma - \alpha = 0$ .

**系 1** 假定  $G \ni a \rightarrow P(a)$  是群  $G$  关于  $n$  級(在  $C$ )矩陣的既約矩陣表現,  $Q \in \mathfrak{M}(n, C)$ . 如果, 对于任意  $a \in G$  有  $P(a)Q = Q \cdot P(a)$ , 那末  $Q = \alpha E_n$  (即  $\mathfrak{A}(C^n)$  集合  $\{P(a); a \in G\}$  的交換子只有  $\alpha E_n$  形状的元)。

**系 2**  $\mathfrak{M}(n, C)$  中与  $GL(n, C)$  (或  $U(n, C)$ ) 的所有元可交換的中元, 只有  $\alpha E_n$  形状的矩陣。

**証明** 由 167 頁例 6 即得。

**定理 4** 可換群的有限次既約表現都是 1 級的。

**証明** 假定  $G$  是可換群,  $\rho$  是它的有限級既約表現,  $V$  是  $\rho$  的表現空間, 那末  $\rho(G) = \{\rho(a); a \in G\} = A$  是既約的  $\mathfrak{A}(V)$  集合。因为  $G$  是可換, 显然  $A \subset A'$ . 由前定理,  $A'$  中元——因而这时所有  $A$  中元——能够表为  $\alpha E_r$  ( $r = \dim V$ ) 的形状, 所以  $r > 1$  就与  $A$  的既約性不合。

**例** 循环群  $Z_m$  的表現。

[解] 由定理 4,  $Z_m$  的有限級既約表現  $\rho$  是 1 級的, 所以

$$\rho: Z_m \rightarrow C^* = C - \{0\},$$

如果把  $Z_m$  的生成元  $1$  的类——用  $a$  表示, 那末

$$Z_m = \{0, a, 2a, \dots, (m-1)a\}, ma = 0.$$

假定  $\rho(a) = \alpha \in C^*$ , 那末  $\alpha^m = 1$ . 即  $\alpha$  必須是 1 的  $m$  次根。又假定 1 的任意  $m$  次根  $\exp 2\pi i k \frac{\sqrt{-1}}{m}$  是  $\alpha_k$  ( $k=0, 1, \dots, m-1$ ), 命

$$\rho_k(a) = \alpha_k, \rho_k(ja) = \alpha_k^j \quad (j=0, 1, \dots, m-1),$$

那末  $\rho_k$  显然給出  $Z_m$  的既約表現。 $Z_m$  具有这  $m$  个既約表現, 其他任意表現是这等既約表現的直和(參照下节)。

## § 27 完全可約表現

假定  $\rho$  是群  $G$  的表現,  $V$  是它的表現空間(參看 § 25), 如果  $W$  是  $V$  的不變子空間, 那末自  $a \in G$  到  $\rho(a)|_W$  的映射, 給出  $G$

的 ( $\dim W$  級) 表現 (定理 1)。它叫做  $\rho$  對於  $W$  的**子表現**, 用  $\rho|W$  來表示。假定  $\dim V = n$ ,  $\dim W_1 = n_1$ ,  $0 < n_1 < n = n_1 + n_2$ , 如果  $(a_1, \dots, a_{n_1})$  是  $W$  的一個基底,  $(a_1, \dots, a_{n_1}, a_{n_1+1}, \dots, a_n)$  是包含它的  $V$  的基底 (§ 5, 定理 5 系 4, 23 頁), 那末由這基底,  $G$  能夠用矩陣表現為

$$G \ni a \rightarrow P(a) = \begin{pmatrix} A(a) & B(a) \\ O_{n_2, n_1} & C(a) \end{pmatrix} \quad (27.1)$$

的形狀。 $a \rightarrow A(a)$  是子表現  $\rho|W$  的矩陣表現。

這時,  $G$  把剩餘空間  $V/W$  作為表現空間的表示, 可以象下面這樣來構成。即  $x \in V$  關於  $\text{mod } W$  的剩餘類  $(x)_W$  確定  $(\rho(a)(x))_W$  (實際上, 假如  $x \equiv y \text{ mod } W$ , 由  $\rho(a)(W) \subset W$  立刻得知  $\rho(a)x \equiv \rho(a)(y) \text{ mod } W$ )。易知  $(x)_W \rightarrow (\rho(a)(x))_W$  是  $GL(V/W)$  中元 (即  $V/W$  到它自身中的映射)。假如  $GL(V/W)$  中元用  $\rho_W(a)$  表示, 那末  $G \ni a \rightarrow \rho_W(a) \in GL(V/W)$  顯然成為  $G$  把  $V/W$  作為表現空間的表現。它叫做  $\rho$  關於  $\text{mod } W$  的**剩餘表現**。

用上面記法,  $(a_{n_1+1})_W, \dots, (a_n)_W$  給出  $V/W$  的一個基底。由這基底  $\rho$  關於  $\text{mod } W$  的矩陣表現是  $a \rightarrow C(a)$  [ $C(a)$  是 (27.1) 中的記法]。

特別,  $[a_{n_1+1}, \dots, a_n] = W'$  也成為不變子空間時,  $\rho$  是直可約,  $V = W \oplus W'$ ,  $\rho = (\rho|W) \oplus (\rho|W')$ , 而剩餘表現  $\rho_W$  與子表現  $\rho|W'$  一致。

不具有子表現的表現不外是既約表現。既約表現的表現空間——即除  $\{0\}$  及自身外不具有不變子空間的表現空間——叫做**既約的**。能夠表為既約表現的直和的表現, 叫做**完全可約的** (既約表現自身也叫做完全可約)。

**定理 5** 下面三個條件是等價的:

(O<sub>1</sub>) 群  $G$  的表現  $\rho$  是完全可約的。

(C<sub>2</sub>)  $\rho$  的表現空間  $V$  是既約表現空間的直和。

(C<sub>3</sub>) 如果  $V$  是  $\rho$  的表現空間,  $W$  是  $V$  的任意不變子空間, 那末  $V$  中就存在滿足  $V = W \oplus W'$  的不變子空間  $W'$ 。

証明 (C<sub>1</sub>)  $\Leftrightarrow$  (C<sub>2</sub>) 是明顯的。

(C<sub>2</sub>)  $\Rightarrow$  (C<sub>3</sub>) 的証明。假定

$$V = V_1 \oplus \cdots \oplus V_r, \quad V_i \text{ 是既約不變子空間 } (i=1, \cdots, r). \quad (27.2)$$

如果  $W$  是  $V$  的不變子空間, 那末  $W \cap V_i = W_i$  也是  $V$  的不變子空間, 因為  $W_i \subset V_i$ ,  $V_i$  是既約, 所以  $W_i = \{0\}$  或  $W_i = V_i$  兩者必有一成立。因此, 如果  $W_i = V_i$ ,  $i=1, \cdots, \nu_1-1$ ,  $W_{\nu_1} = \{0\}$  (即如果  $W \supset V_1, \cdots, V_{\nu_1-1}$ ,  $W \cap V_{\nu_1} = \{0\}$ ), 那末  $W \oplus V_{\nu_1}$  被定義, 顯然它成為  $V$  的不變子空間。又  $W \oplus V_{\nu_1} \supset V_i$ ,  $i=1, \cdots, \nu_1$ .  $W \oplus V_{\nu_1}$  顯然都是  $V$  的不變子空間, 現在與考察  $W$  一樣來考察  $W \oplus V_{\nu_1}$ , 那末  $W \oplus V_{\nu_1} \supset V_i$ ,  $i=\nu_1+1, \cdots, \nu_2-1$ ,  $(W \oplus V_{\nu_1}) \cap V_{\nu_2} = \{0\}$  這樣的番號  $\nu_2$  確定, 而  $W \oplus V_{\nu_1} \oplus V_{\nu_2}$  成為  $V$  的不變子空間, 並且  $\supset V_i$ ,  $i=1, \cdots, \nu_2$ . 繼續這樣下去, 最後得到

$$W \oplus V_{\nu_1} \oplus V_{\nu_2} \oplus \cdots \oplus V_{\nu_k} \supset V_i \quad (i=1, \cdots, \nu).$$

於是  $V \supset W \oplus V_{\nu_1} \oplus \cdots \oplus V_{\nu_k} \supset V_1 \oplus \cdots \oplus V_\nu = V$ .

所以  $W \oplus V_{\nu_1} \oplus \cdots \oplus V_{\nu_k} = V$ .

因此命  $W' = V_{\nu_1} \oplus \cdots \oplus V_{\nu_k}$  即得。

(C<sub>3</sub>)  $\Rightarrow$  (C<sub>2</sub>) 的証明。假如  $V$  自身是既約, 那就好了。假如  $V$  是可約, 如果  $V_1$  是  $V$  的最小維的不變子空間, 那末  $V_1$  顯然是既約。對於  $W = V_1$  引用 (C<sub>3</sub>) 就得到滿足  $V = V_1 \oplus V'_1$  的不變子空間  $V'_1$ . 假如  $V'_1$  是既約, 那就好了。如果又是可約, 命含於  $V'_1$  的最小維的不變子空間是  $V_2$ , 那末  $V_2$  是既約。再對於  $W = V_1 \oplus V_2$  引用 (C<sub>3</sub>) 就得到  $V = V_1 \oplus V_2 \oplus V'_2$ . 繼續這個方法能夠得到象 (27.2) 那樣的直和分解。 (証畢)

表現空間  $V$  滿足上面的條件 (C<sub>2</sub>) 或 (C<sub>3</sub>) 時, 叫做完全可約。

这时  $V$  不外是某完全可約表現的表現空間。下面系的証明包含在上定理的証明中。

**系** 假定  $V$  是群  $G$  的完全可約表現空間, 如果

$$V = V_1 \oplus V_2 \oplus \cdots \oplus V_r,$$

是  $V$  的既約不變子空間的直和分解, 那末对于  $V$  的任意不變子空間  $W$ , 能够自  $V_1, \dots, V_r$  中适当的挑选  $V_{n_1}, \dots, V_{n_k}$ , 使

$$W = V_{n_1} \oplus \cdots \oplus V_{n_k}. \quad (\text{系毕})$$

由定理 5 及它的系, 象下面所示能够导出如下的定理。

**定理 6** 假定  $\rho$  是群  $G$  的完全可約表現, 如果

$$\rho = \kappa_1 \oplus \cdots \oplus \kappa_r = \kappa'_1 \oplus \cdots \oplus \kappa'_{r'},$$

是  $\rho$  的两种既約表現的直和分解, 那末  $r = r'$ , 如果必要, 适当排列  $\kappa'_1, \dots, \kappa'_{r'} = \kappa'_r$ , 能够使  $\kappa_1 \sim \kappa'_1, \dots, \kappa_r \sim \kappa'_r$  ( $\sim$  为等价表現 (参照 § 25))。 (定理毕)

当  $\rho_1, \rho_2$  是  $G$  的等价表現时,  $\rho_1$  的表現空間  $V_1$  与  $\rho_2$  的表現空間  $V_2$  叫做作为表現空間的同构, 用  $V_1 \sim V_2$  表示。(所謂  $V_1, V_2$  是表現空間是有自  $G$  到  $GL(V_1), GL(V_2)$  的同态映射—— $G$  的表現—— $\rho_1, \rho_2$  而  $V_1, V_2$  分别是  $\rho_1, \rho_2$  的表現空間。) 假如  $V_1, V_2$  是  $G$  的同构表現空間, 那末对于任意  $x \in G$ , 有自  $V_1$  到  $V_2$  滿足

$$f \circ \rho_1(x) = \rho_2(x) \circ f$$

的(作为向量空間的)同构映射  $f$ . 这  $f$  叫做自  $V_1$  到  $V_2$  作为表現空間的同构映射(用这种叙述方法, “作为表現空間”这話, 当  $V_1, V_2$  显然是表現空間时, 有时省略)。定理 6 就表現空間来叙述, 就成为下面的定理。

$$\begin{array}{ccc} V_1 & \xrightarrow{\rho_1(x)} & V_1 \\ f \downarrow & & \downarrow f \\ V_2 & \xrightarrow{\rho_2(x)} & V_2 \end{array}$$

**定理 6'** 假定  $V$  是群  $G$  的完全可約表現空間, 如果

$$V = V_1 \oplus \cdots \oplus V_r = V'_1 \oplus \cdots \oplus V'_{r'}. \quad (27.3)$$

是  $V$  的两种既約不變子空間的直和分解, 那末  $r = r'$  并且如果必



要,适当排列  $V'_1, \dots, V'_r = V'_r$ , 能够使  $V_i \sim V'_i (i=1, \dots, r)$ .

**証明** 依定理 6' 的形式, 用关于  $r$  的归纳法来証明。

当  $r=1$  时, 假如  $r' > 1$ , 那末  $V'_1 \subseteq V = V_1$ . 这与  $V_1$  是既約的假定矛盾。所以  $r'=1$ , 于是  $V = V_1 = V'_1$ . 因此, 当然  $V_1 \sim V'_1$ .

直和因子个数是  $r-1$  时, 假定其成立, 来証明直和因子个数是  $r$  时亦成立。假定  $r' \geq r$ . 命  $V'_1 \oplus \dots \oplus V'_{r-1} = W'$ , 由定理 5 的系,  $V = W' \oplus W$ , 而  $W$  是几个  $V_i$  的直和。因为  $W \sim V/W' \sim V'_r$ ,  $V'_r$  是既約, 所以  $W$  与  $V_i$  中某一个同构。如果  $W \sim V_r$ , 那末  $W' = V'_1 \oplus \dots \oplus V'_{r-1} \sim V/W \sim V/V_r \sim V_1 \oplus \dots \oplus V_{r-1}$ . 由这同构对应, 假如  $V_1, \dots, V_{r-1}$  到  $W'$  內的象是  $V''_1, \dots, V''_{r-1}$ , 那末

$W' = V'_1 \oplus \dots \oplus V'_{r-1} = V''_1 \oplus \dots \oplus V''_{r-1}$ ,  $V''_i \sim V_i (i=1, \dots, r-1)$ . 这是  $W'$  关于既約不变子空間的两种直和分解, 因为  $r-1 \leq r'-1$ , 所以由归纳法的假定,  $r-1 = r'-1$ , 并且适当改换番号, 能成为

$$V_i \sim V'_i \quad (i=1, \dots, r-1).$$

因此  $r=r'$ ,  $V_i \sim V'_i \quad (i=1, \dots, r)$ . (証毕)

**注意** 实际上, 有下面更一般的定理 (Jordan, Hölder-E. Noether)。

假定  $V$  是群  $G$  的任意表現空間 (不一定是完全可約)。这时作  $V$  的不变子空間列

$$V_0 = \{0\} \subset V_1 \subset V_2 \subset \dots \subset V_r = V, \quad (1)$$

使得商空間  $W_i = V_i/V_{i-1}$ ,  $i=1, \dots, r$  都是既約。于(1)之外, 如果

$$V'_0 = \{0\} \subset V'_1 \subset V'_2 \subset \dots \subset V'_{r'} = V \quad (1')$$

是与(1)同种类的列 ( $W'_j = V'_j/V'_{j-1}$ ,  $j=1, \dots, r'$  都是既約), 那末  $r=r'$ , 并且取  $1, \dots, r$  的适当排列  $\nu_1, \dots, \nu_r$ , 能够使  $W_1 \sim W'_{\nu_1}, \dots, W_r \sim W'_{\nu_r}$ .

因为象后面定理 8 系所示, 有限群的表现都是完全可約的, 所以我們不做这一般情况的証明, 而只証明定理 6。

象在本章开始所申明的那样, 表現空間  $V$  的基础体假定是复数体  $C$ , 因此由第 1 章 § 17 所示, 能够于  $V$  导入內积  $(x, y)$  来考虑  $V$  的酉变换, 即使內积不变的变换。  $V$  的酉变换全体成为  $GL(V)$

的子群(第2章 § 22 例 7, 146 頁), 用  $U(V)$  表示。把  $V$  作为表現空間的群  $G$  的表現  $\rho$  是自  $G$  到  $GL(V)$  的同態映射。特別, 它的象  $\rho(G)$  在  $U(V)$  中時, 即  $\rho$  成为自  $G$  到  $U(V)$  的同態映射時,  $\rho$  叫做  $G$  的(把  $V$  作为表現空間, 关于內积  $(x, y)$  的)酉表現。当  $\rho$  是酉表現時, 如果取  $V$  的正規直交坐标系, 那末  $\rho(a)$ ,  $a \in G$ , 能够用酉矩陣  $P(a)$  表示(第1章 § 17, 102 頁)。反之, 对于  $V$  的某坐标系, 表示  $\rho(a)$ ,  $a \in G$  的矩陣  $P(a)$  如果都是酉矩陣, 那末  $\rho$  显然成为酉表現。

**定理 7** 酉表現是完全可約的。

**証明** 假定  $\rho$  是酉表現,  $V$  是它的表現空間, 对于  $V$  的任意  $\rho$  的不變子空間  $W$ , 証明有滿足  $V = W \oplus W'$  的  $\rho$  的不變子空間  $W'$  (定理 5) 即可。假定  $W' = \{x'; x' \perp W\}$ , 由第1章 § 16 定理 21 得  $V = W \oplus W'$ 。又因为  $\rho$  是酉表現, 所以对于任意  $x \in W$ ,  $x' \in W'$ ,  $a \in G$  有  $(x, \rho(a)(x')) = (\rho(a^{-1})(x), x')$ 。因为  $W$  是不變子空間, 所以  $\rho(a^{-1})(x) \in W$ , 又因为  $x' \perp W$ , 所以  $(\rho(a^{-1})(x), x') = 0$ 。于是  $(x, \rho(a)(x')) = 0$ , 即  $\rho(a)(x') \in W'$ 。因此  $W'$  是不變子空間。

**定理 8** 有限群的表現(关于表現空間的适当內积)是酉表現。

**証明** 假定  $G$  是阶为  $n$  的有限群,  $\rho$  是  $G$  的表現,  $V$  是  $\rho$  的表現空間。对于  $x, y \in V$ , 它的內积  $(x, y)$  是  $C$  中元, 命

$$\langle x, y \rangle = \frac{1}{n} \sum_{a \in G} (\rho(a)(x), \rho(a)(y)),$$

容易驗證  $\langle x, y \rangle$  是  $V$  的另一个內积(驗證第1章 § 17 的条件 U1~5 即可)。并且对于  $G$  的任意元  $b$ ,

$$\begin{aligned} \langle \rho(b)(x), \rho(b)(y) \rangle &= \frac{1}{n} \sum_{a \in G} (\rho(a)(\rho(b)(x)), \rho(a)(\rho(b)(y))) \\ &= \frac{1}{n} \sum_{a \in G} (\rho(ab)(x), \rho(ab)(y)) = \langle x, y \rangle. \end{aligned}$$

(自第二边变为第三边时, 是因为  $\rho$  是表现, 引用了  $\rho(a)\rho(b) = \rho(ab)$  这结果。又自第三边变为第四边时, 因为  $G$  是群, 引用了对于一定的  $b \in G$ , 当  $a$  取  $G$  中每一元时,  $ab$  也同样取全部  $G$  中元这事实)。

即  $\rho(b)$ ,  $b \in G$ , 不变内积  $\langle x, y \rangle$ . 所以  $\rho$  (关于内积  $\langle x, y \rangle$ ) 是酉表现。

**系** 有限群的表现是完全可约的。

**証明** 由定理 7 及 8 即得。

由这系, 求有限群  $G$  的表现的问题归结为求  $G$  的所有既约表现的问题。这问题将在后面解决(参照 § 33)。

**例 1** 因为可换群的既约表现都是 1 级的(定理 4), 所以表现有限可换群的矩阵都能够变为对角线型。

**例 2** 求对称群  $\mathfrak{S}_3 = \mathfrak{S}(\{1, 2, 3\})$  的既约表现(以后对称群  $\mathfrak{S}(\{1, 2, \dots, n\})$  简单地用  $\mathfrak{S}_n$  表示)。

[解] 一般, 对于  $G = \mathfrak{S}_n$  中元  $\begin{pmatrix} 1 & 2 & \cdots & n \\ \nu_1 & \nu_2 & \cdots & \nu_n \end{pmatrix}$  使与  $\pi(\nu_1, \dots, \nu_n) \in GL(C^n)$

(29 頁, 例 6) 对应, 就得到  $G$  的一个  $n$  级忠实表现  $\rho$ . 把  $C^n$  的自然基底  $(e_1, \dots, e_n)$  看成正規直交基底时,  $C^n \ni x = \sum_{i=1}^n \xi_i e_i, y = \sum_{i=1}^n \eta_i e_i$  的内积为

$$(x, y) = \sum_{i=1}^n \xi_i \bar{\eta}_i,$$

因为  $(\pi(\nu_1, \dots, \nu_n)x, \pi(\nu_1, \dots, \nu_n)y) = \sum_{i=1}^n \xi_{\nu_i} \bar{\eta}_{\nu_i} = (x, y),$

所以  $\rho$  是酉表现。

当  $n=3$  时, 試将这表示  $\rho$  分解为既约表示的直和。显然  $C^3 = C^3$  具有用  $e_1 + e_2 + e_3$  生成的空間作为不变子空間, 为了正規化, 命

$$\frac{1}{\sqrt{3}}(e_1 + e_2 + e_3) = f_1,$$

如果  $f_2 = \frac{1}{\sqrt{3}}\left(\sqrt{2}e_1 - \frac{1}{\sqrt{2}}e_2 - \frac{1}{\sqrt{2}}e_3\right), f_3 = \frac{1}{\sqrt{2}}(e_2 - e_3),$

那末  $(f_1, f_2, f_3)$  成为  $C^3$  的正規直交基底。显然  $\pi(\nu_1, \nu_2, \nu_3)(f_1) = f_1$ , 所以  $\rho$

对于不变子空間  $[f_1]$  的子表現  $\rho_1$  是恒等表現。因为  $[f_2, f_3] = \{x; x \perp f_1\}$ , 所以  $[f_2, f_3]$  也是  $C^3$  的不变子空間。假如  $\rho$  对于这不变子空間的子表現是  $\rho_2$ , 那末  $\rho = \rho_1 \oplus \rho_2$ .

試求表現  $\rho_2$  由基底  $(f_2, f_3)$  的表現矩陣。

假定对換  $(1, 2) = a, (1, 3) = b$ , 因为  $G = \{e, a, b, ab, ba, aba\}$ , 所以, 如果  $\rho_2(a), \rho_2(b)$  已知, 那末  $\rho_2(ab) = \rho_2(a)\rho_2(b)$  等也能求得。取  $C^3$  的自然基底, 那末  $\rho(a), \rho(b)$  分別用

$$P(1\ 2) = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad P(1\ 3) = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$$

表示, 因为自然基底到  $(f_1, f_2, f_3)$  的坐标变换的矩陣是

$$Q = \begin{pmatrix} \frac{1}{\sqrt{3}} & \sqrt{\frac{2}{3}} & 0 \\ \frac{1}{\sqrt{3}} & -\frac{1}{\sqrt{6}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{3}} & -\frac{1}{\sqrt{6}} & -\frac{1}{\sqrt{2}} \end{pmatrix},$$

所以  $\rho(a), \rho(b)$  由坐标系  $(f_1, f_2, f_3)$  表示的矩陣是

$$Q^{-1}P(1\ 2)Q = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -\frac{1}{2} & \frac{\sqrt{3}}{2} \\ 0 & \frac{\sqrt{3}}{2} & \frac{1}{2} \end{pmatrix}, \quad Q^{-1}P(1\ 3)Q = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -\frac{1}{2} & -\frac{\sqrt{3}}{2} \\ 0 & \frac{\sqrt{3}}{2} & \frac{1}{2} \end{pmatrix}.$$

于是  $\rho_2(a), \rho_2(b)$  由  $(f_2, f_3)$  表示的矩陣分別为

$$\begin{pmatrix} -\frac{1}{2} & \frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & \frac{1}{2} \end{pmatrix}, \quad \begin{pmatrix} -\frac{1}{2} & -\frac{\sqrt{3}}{2} \\ -\frac{\sqrt{3}}{2} & \frac{1}{2} \end{pmatrix}.$$

因为  $\rho_2$  是 2 級表現, 所以它是既約的。实际上, 假如  $\rho_2$  是可約, 那就不得不成为两个 1 級表現  $\rho'_2, \rho''_2$  的直和。但对于 1 級表現, 可換性  $\rho'_2(a)\rho'_2(b) = \rho'_2(b)\rho'_2(a)$ ,  $\rho''_2(a)\rho''_2(b) = \rho''_2(b)\rho''_2(a)$  成立, 因此不得不  $\rho_2(a)\rho_2(b) = \rho_2(b)\rho_2(a)$ , 这与上面的事实不合。

$\mathfrak{S}_3$  的既約表現, 实际上, 除  $\rho_1, \rho_2$  外还有一个交代表現  $\rho_3, \rho_3$  不与  $\rho_1, \rho_2$  中任一个等价。 $\mathfrak{S}_3$  的既約表現只有这三个, 这将在后面証明 (§33)。而一般全部求对称群  $\mathfrak{S}_n$  的既約表現的問題将在 §38~§41 完全解决。

### §28 反步表現, 張量积表現

象以前一样, 假定  $\rho$  是群  $G$  的表現,  $V$  是  $\rho$  的表現空間,  $\hat{V}$  是  $V$  的对偶空間, 对于  $GL(V)$  中元  $\rho(a)$ , 如果使  $GL(\hat{V})$  中元  ${}^t\rho(a)$  与之对应(第1章 §10), 因为  $\rho$  是表現, 所以

$$\rho(ab) = \rho(a)\rho(b),$$

但关于  ${}^t\rho$ ,

$${}^t\rho(ab) \neq {}^t(\rho(a)\rho(b)) = {}^t\rho(b){}^t\rho(a),$$

因此, 如果  $G$  不是可換群, 那末  ${}^t\rho$  一般不能成为  $G$  的表現。

又对于  $a \in G$ , 如果使  $\rho(a^{-1}) \in GL(V)$  对应, 那就得到自  $G$  到  $GL(V)$  的映射。假如它用  $\hat{\rho}$  表示, 那末

$$\hat{\rho}(ab) = \rho(b^{-1}a^{-1}) = \hat{\rho}(b)\hat{\rho}(a),$$

因此  $\hat{\rho}$  一般也不能成为  $G$  的表現。但是, 如果命

$${}^t\hat{\rho}(a) = {}^t\rho(a^{-1}) = \rho^*(a),$$

那末  $\rho^*$  显然給出把  $\hat{V}$  作为表現空間的  $G$  的表現:

$$\rho^*(ab) = {}^t\rho(b^{-1}a^{-1}) = \rho^*(a)\rho^*(b).$$

$\rho^*$  叫做  $\rho$  的**反步表現**。假如取  $V$  的坐标的对偶坐标作为  $\hat{V}$  的坐标, 那末  $\rho^*$  的表現矩陣  $P^*(a)$  能够由  $\rho$  的表現矩陣  $P(a)$  得出:

$$P^*(a) = {}^tP(a^{-1}).$$

**例1** 在表現  $\rho$  中,  $\rho(a), a \in G$  都是直交变换时,  $\rho$  叫做**直交表現**。表現  $\rho, \rho^*$  对于对偶坐标系能够用相同的矩陣来表現的必要充分条件是  $\rho$  为直交表現。

[解]  $P^*(a) = ({}^tP(a))^{-1}$ , 所以  $P(a) = P^*(a) \Leftrightarrow P(a){}^tP(a) = E$ . 因此本例显然成立。

假定  $\rho_1, \rho_2$  是群  $G$  的两个表現, 它的表現空間分別是

$V_1, V_2$ . 于是, 对于  $a, b \in G$ ,  $\rho_1(a) \otimes \rho_2(a), \rho_1(b) \otimes \rho_2(b)$  都是  $V_1 \otimes V_2$  的自同构映射, 但  $(\rho_1(a) \otimes \rho_2(a)) \cdot (\rho_1(b) \otimes \rho_2(b)) = \rho_1(a) \cdot \rho_1(b) \otimes \rho_2(a) \cdot \rho_2(b)$  (第 1 章 § 20 例 8)。因此, 如果命  $\rho_1(a) \otimes \rho_2(a) = \rho(a)$ , 那末  $a \rightarrow \rho(a)$  成为把  $V_1 \otimes V_2$  作为表现空间的  $G$  的表现。它叫做  $\rho_1, \rho_2$  的张量积表现, 写成  $\rho = \rho_1 \otimes \rho_2$ 。

**例 2**  $\rho_1 \otimes \rho_2$  的级数等于  $\rho_1, \rho_2$  的级数的积。

**例 3** 假定  $\varphi_1, \varphi_2$  是  $V_1, V_2$  的坐标系, 如果  $P_1(a), P_2(a)$  是对于这等坐标系表现  $\rho_1(a), \rho_2(a)$  的矩阵, 象在第 1 章 § 20 所看到的一样, 对于  $V_1 \otimes V_2$  的坐标系  $\varphi_1 \otimes \varphi_2$ ,  $\rho_1(a) \otimes \rho_2(a)$  能够用矩阵  $P_1(a) \otimes P_2(a)$  表示。在这意义下, 张量积表现的表现矩阵是各因子的表现矩阵的张量积。

**例 4** 关于表现的张量积, 结合律成立, 即

$$(\rho_1 \otimes \rho_2) \otimes \rho_3 = \rho_1 \otimes (\rho_2 \otimes \rho_3).$$

它简单地推广成  $\rho_1 \otimes \rho_2 \otimes \rho_3$ . 关于四个以上的表现也同样能够定义  $\rho_1 \otimes \rho_2 \otimes \cdots \otimes \rho_n$  (参照第 1 章 § 20, 命题 63, 128 页)。

**例 5** 直和表现与张量积表现之间在下面的意义下, 有分配律成立 (第 1 章 § 20 例 7, 129 页)。

$$\rho_1 \otimes (\rho_2 \oplus \rho_3) = (\rho_1 \otimes \rho_2) \oplus (\rho_1 \otimes \rho_3),$$

$$(\rho_1 \oplus \rho_2) \otimes \rho_3 = (\rho_1 \otimes \rho_3) \oplus (\rho_2 \otimes \rho_3).$$

## § 29 群代数与正则表现

假定  $G$  是群, 对于把  $G$  作为定义域,  $C$  作为值域的全体函数 (参照 § 6) 的集合  $A(G)$ , 能够如下地构造成为  $C$  上代数 (§ 7, 32 页)。

首先, 对于  $f, g \in A(G), a \in G, \lambda \in C$ , 由

$$(f+g)(a) = f(a) + g(a),$$

$$(\lambda f)(a) = \lambda f(a),$$

定义  $f+g, \lambda f \in A(G)$ , 显然  $A(G)$  成为  $C$  上向量空间 (参照 32 页命题 5 的证明)。特别, 假如  $G$  是  $n$  阶有限群, 那末这向量空间的维数是  $n$ , 对于  $G$  中各元  $a$ , 由

$$f_a(x) = \begin{cases} 1, & a = x \text{ 时}, \\ 0, & a \neq x \in G \text{ 时} \end{cases} \quad (29.1)$$

定义的  $A(G)$  中  $n$  个元的集合  $\{f_a; a \in G\}$  成为  $A(G)$  的一个基底。实际上,任意  $f \in A(G)$  能够写成

$$f = \sum_{a \in G} f(a) f_a, \quad (29.2)$$

反之,假如  $f = \sum_{a \in G} \lambda_a f_a$ , 那末  $\lambda_a = f(a)$ , 这由 (29.1) 立即明白。

其次,这基底中元  $f_a, f_b, a, b \in G$  之間的乘法由

$$f_a \cdot f_b = f_{ab} \quad (29.3)$$

定义(在这里用了群的公理 1), 于是 (29.2) 定义的  $f$  与

$$g = \sum_{a \in G} g(a) f_a \quad (29.4)$$

的积(为了使  $A(G)$  成为代数),就必须规定为

$$\begin{aligned} fg &= (\sum f(a) f_a) (\sum g(b) f_b) \\ &= \sum_{a, b \in G} f(a) g(b) f_{ab} \\ &= \sum_{a \in G} (\sum_{b \in G} f(ab^{-1}) g(b)) f_a. \end{aligned} \quad (29.5)$$

又由此规定,容易验证  $A(G)$  是  $C$  上代数(特别  $A(G)$  的乘法满足结合律,能够由  $G$  所满足的群公理 3 导出)。这样考虑了代数构造的  $A(G)$ , 叫做  $G$  上群代数。

再,  $K$  是任意体时,用  $K$  来代替  $C$ , 与上完全一样能够定义  $K$  上 ( $G$  上的) 群代数  $A(G, K)$ , 这也是代数学上常用的一个概念。以下为了简单起见, 如果不加声明, 群代数的基础体假定是  $C$ 。

**例 1**  $f_e$  ( $e$  是  $G$  的单位元) 是  $A(G, K)$  中乘法的单位元:  $f_e f = f f_e = f$ 。

**例 2** (29.5) 的右边也能够象下面这样写出:

$$\sum_{b \in G} (\sum_{a \in G} f(a) g(a^{-1}b)) f_b.$$

**例 3** 在两个代数  $A, B$  作为向量空间的直和中, 如果由法则

$$(a_1 \oplus b_1)(a_2 \oplus b_2) = (a_1 a_2 \oplus b_1 b_2)$$

导入乘法就成为代数。它叫做代数  $A, B$  的直和, 用  $A \oplus B$  表示。假如  $G$  是 4 阶循环群,  $K = R$ , 那末  $A(G, R)$  与直和  $R \oplus R \oplus R$  同构。

**例 4** 假定  $G$  是由八个元  $\{\pm 1, \pm i, \pm j, \pm k\}$  构成的群, 它的乘法用  $i^2 = j^2 = k^2 = -1, ij = -ji = k, jk = -kj = i, ki = -ik = j$  ( $1$  是单位元) 给出。这群叫做 **四元数群** (quaternion group)。  $R$  上 4 元数环 (33 页) 如果是  $Q(R)$ , 那就能够证明  $A(G, R)$  与  $R \oplus R \oplus R \oplus R \oplus Q(R)$  同构。

一般, 在有单位元的代数  $A$  中, 关于乘法有逆元的元叫做 **正则元**。假定  $A$  中正则元全体的集合是  $A^*$ , 那末  $A^*$  关于乘法显然成群, 特别由  $A(G)$  中正则元形成的群用  $A^*(G)$  表示。

**命题 4**  $f_a \in A^*(G)$ 。

**证明** 因为  $f_a f_{a^{-1}} = f_e$ , 所以  $f_a^{-1} = f_{a^{-1}}$ 。即  $f_a$  有逆元  $f_{a^{-1}}$ , 所以它是正则元。

**命题 5** 对于  $a \in G$ , 使  $f_a \in A^*(G)$  对应的映射  $\iota$  是自  $G$  到  $A^*(G)$  中的同构映射 (同态单射)。

**证明** 由定义 (29.3) 自明。 (证毕)

由这命题 5 把  $a$  与  $\iota(a) = f_a$  同样看待, 那末  $f = \sum f(a) f_a$  有时写成  $f = \sum f(a) a$ 。

**例 5** 假定  $\rho$  是  $G$  的任意表现,  $V$  是它的表现空间, 那末对于任意  $a \in G$ , 有  $\rho(a) \in \mathfrak{L}(V)$ , 如果把  $A(G)$  中元  $f_a$  与  $a$  同样看待, 那末, 对于  $a \in A(G)$  也能认为有  $\rho(a) \in \mathfrak{L}(V)$ 。这时, 对于  $A(G)$  中任意元  $f = \sum f(a) a$ , 假如定义  $\rho(f) = \sum_{a \in G} f(a) \rho(a) \in \mathfrak{L}(V)$ , 那末  $\rho$  就成为自  $A(G)$  到  $\mathfrak{L}(V)$  作为代数的同态映射 (后面  $\rho$  的定义域 (对于开始  $\rho$  的定义域  $G$  的) 扩张到  $A(G)$ , 如果不致引起混淆, 一般可以用相同文字  $\rho$  表示)。

**定理 9** 假定  $G$  是有限群,  $A$  是  $C$  上任意具有单位元的代数, 如果  $\varphi$  是自  $G$  到  $A$  中正则元形成的群  $A^*$  的同态映射。那就存在满足下面条件的自  $G$  上代数  $A(G)$  到  $A$  作为代数的同态映射  $\Phi$ 。

$$\begin{array}{ccc} G & \xrightarrow{\varphi} & A^* \\ & \searrow \iota & \uparrow \phi^* \\ & & A^*(G) \end{array}$$

假如把  $\Phi$  到  $A^*(G)$  的缩小作为  $\Phi^*$ , 则



$$\varphi = \Phi^* \circ \iota. \quad (29.6)$$

**証明**  $\Phi$  象下面这样构造即可。因为  $\{f_a; a \in G\}$  是  $A(G)$  的基底, 所以  $\Phi(f_a) \in A$  可以任意规定, 如果, 对于  $f = \sum f(a)f_a$ , 使  $\Phi(f) = \sum f(a) \cdot \Phi(f_a)$  对应, 那就得到自  $A(G)$  到  $A$  作为向量空间的同态映射。这时, 假如  $\Phi(fg) = \Phi(f)\Phi(g)$ , 那末  $\Phi$  也给出作为代数的同态。这容易理解, 只要关于基底  $\Phi(f_a), \Phi(f_b), \dots$  之間乘法的同态关系

$$\Phi(f_a)\Phi(f_b) = \Phi(f_{ab}) \quad (29.7)$$

成立就可以。現在命  $\Phi(f_a) = \varphi(a)$ , 由  $\varphi$  是同态映射的假定, (29.7) 成立是显然的。又因为  $f_a = \iota(a)$ , 所以 (29.6) 也当然成立。  
(証毕)

当  $G$  的阶是  $n$  时,  $A(G)$  是  $C$  上的  $n$  維向量空間, 对于  $a \in G, f \in A(G)$ , 假如由 ①

$$\begin{aligned} (\rho(a)f)(x) &= f(a^{-1}x), \\ (\sigma(a)f)(x) &= f(xa) \end{aligned}$$

定义  $\rho(a): A(G) \rightarrow A(G), \sigma(a): A(G) \rightarrow A(G)$ , 显然  $\rho(a), \sigma(a) \in \mathfrak{B}(A(G))$ , 并且

$$\begin{aligned} (\rho(a)\rho(b^{-1})f)(x) &= (\rho(b^{-1})f)(a^{-1}x) = f(ba^{-1}x), \\ (\rho(ab^{-1})f)(x) &= f((ab^{-1})^{-1}x) = f(ba^{-1}x), \end{aligned}$$

于是  $\rho(a)\rho(b^{-1}) = \rho(ab^{-1})$ , 所以  $\rho$  成为把  $A(G)$  作为表現空間的  $G$  的表現。同样  $\sigma$  也成为把  $A(G)$  作为表現空間的  $G$  的另一表現。 $\rho$  叫做  $G$  的左正則表現,  $\sigma$  叫做  $G$  的右正則表現。

**定理 10** 有限群  $G$  的左正則表現  $\rho$  与右正則表現  $\sigma$  同是忠实表現, 并且是相互等价的。

---

①  $\rho(a)f$  的定义不是把  $a^{-1}x$  代入  $f(x)$  中的  $x$  作为  $(\rho(a)f)(x)$ , 而是“ $\rho(a)f$  在  $x$  的值等于  $f$  在  $a^{-1}x$  的值”这个意义, 象后面所看到的变形  $(\rho(a)f)(bx) = f(a^{-1}bx)$  那样。关于  $\sigma$  也是同样。

**证明** 假定  $\rho(a) = e_{A(G)}$ , 那末对于任意  $f \in A(G)$  有  $f(a^{-1}x) = f(x)$ . 如果  $a \neq e$ , 取  $f_e$  作为  $f$ ,  $a$  作为  $x$ , 就产生  $1=0$  这样的矛盾, 所以  $a=e$ . 即  $\text{Ker } \rho = \{e\}$ . 因此  $\rho$  是忠实的。关于  $\sigma$  也是同样。

其次, 为了证明  $\rho, \sigma$  等价, 用

$$\pi f(x) = f(x^{-1})$$

$$\begin{array}{ccc} A(G) & \xrightarrow{\rho(a)} & A(G) \\ \pi \downarrow & & \downarrow \pi \\ A(G) & \xrightarrow{\sigma(a)} & A(G) \end{array}$$

定义

$$\pi: A(G) \rightarrow A(G).$$

显然  $\pi$  是同构映射。这时由上面的图可见它更是可换的, 即

$$\pi \circ \rho(a) = \sigma(a) \circ \pi. \quad (29.8)$$

实际上,

$$\begin{aligned} (\pi \circ \rho(a)f)(x) &= (\pi(\rho(a)f))(x) = (\rho(a)f)(x^{-1}) = f(a^{-1}x^{-1}), \\ ((\sigma(a) \circ \pi)f)(x) &= (\sigma(a)(\pi f))(x) \\ &= (\pi f)(xa) = f((xa)^{-1}) = f(a^{-1}x^{-1}), \end{aligned}$$

因此  $\rho \sim \sigma$ .

**例 6** 依照命题 5, 如果把  $f_x$  写成  $a$ , 那末  $\{e, a, b, \dots, x, \dots\}$  成为  $A(G)$  的基底。显然  $\rho(a)f_x = f_{ax}$ <sup>①</sup>, 所以用这基底时, 表示  $\rho(a)$  的矩阵是表示排列  $\begin{pmatrix} e & a & b & \dots & x & \dots \\ a^{-1} & e & a^{-1}b & \dots & a^{-1}x & \dots \end{pmatrix}$  的  $n$  级矩阵 (37 页)。同样,  $\sigma(a)$  能够用表示排列  $\begin{pmatrix} e & a & b & \dots & x & \dots \\ e & a^{-1} & ba & \dots & xa & \dots \end{pmatrix}$  的矩阵表现。又, 上面的  $\pi \in \mathfrak{L}(A(G), A(G))$ , 能够用表示排列  $\begin{pmatrix} e & a & b & \dots & x & \dots \\ e & a^{-1} & b^{-1} & \dots & x^{-1} & \dots \end{pmatrix}$  的矩阵表现, 这些排列 (或表示它的矩阵) 简单地分别用  $\begin{pmatrix} x \\ a^{-1}x \end{pmatrix}$ ,  $\begin{pmatrix} x \\ xa \end{pmatrix}$ ,  $\begin{pmatrix} x \\ x^{-1} \end{pmatrix}$  表示。(上面的 (29.8) 用这记法意味着

$$\begin{pmatrix} x \\ x^{-1} \end{pmatrix} \begin{pmatrix} x \\ a^{-1}x \end{pmatrix} = \begin{pmatrix} x \\ xa \end{pmatrix} \begin{pmatrix} x \\ x^{-1} \end{pmatrix},$$

这也容易直接证明。)

<sup>①</sup> 因为  $(\rho(a)f_x)(y) = f_x(a^{-1}y) = \begin{cases} 1, & \text{当 } y=ax \\ 0, & \text{当 } y \neq ax \end{cases}$  而  $f_{ax}(y) = \begin{cases} 1, & \text{当 } y=ax \\ 0, & \text{当 } y \neq ax \end{cases}$   
所以  $\rho(a)f_x = f_{ax}$ . — 译者注

$e$	$a^{-1}$	$b^{-1}$	$\dots$	$x^{-1}$	$\dots$
$a$	$e$	$ab^{-1}$	$\dots$	$ax^{-1}$	$\dots$
$b$	$ba^{-1}$	$e$	$\dots$	$bx^{-1}$	$\dots$
$\vdots$	$\vdots$	$\vdots$		$\vdots$	
$x$	$xa^{-1}$	$xb^{-1}$	$\dots$	$e$	$\dots$
$\vdots$	$\vdots$	$\vdots$		$\vdots$	

(a)

$e$	$a^{-1}$	$b^{-1}$	$\dots$	$x^{-1}$	$\dots$
$a$	$e$	$b^{-1}a$	$\dots$	$x^{-1}a$	$\dots$
$b$	$a^{-1}b$	$e$	$\dots$	$x^{-1}b$	$\dots$
$\vdots$	$\vdots$	$\vdots$		$\vdots$	
$x$	$a^{-1}x$	$b^{-1}x$	$\dots$	$e$	$\dots$
$\vdots$	$\vdots$	$\vdots$		$\vdots$	

(b)

上面由群  $G$  中元形成的 (a), (b) 那样的表叫做  $G$  的群表, (a) 叫做左群表, (b) 叫做右群表。(也可以說是群  $G$  的乘法表。) 表示  $\rho(a)$  的矩陣在左表中命  $a$  的地方为 1, 其他地方为 0 即得<sup>①</sup>。表示  $\sigma(a)$  的矩陣在右表中命  $a^{-1}$  的地方为 1, 其他地方为 0 即得。

例 7 取例 6 的基底时,  $n$  阶循环群的正则表示为下面的矩陣形式

$$\begin{pmatrix} 1 & & & & \\ & 1 & & & \\ & & \ddots & & \\ & & & 1 & \\ 0 & & & & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & & & \\ & 0 & 1 & & \\ & & 0 & 1 & \\ & & & 0 & 1 \\ 1 & 0 & & & 0 \end{pmatrix}, \dots, \begin{pmatrix} 0 & & & 0 & 1 \\ & 1 & 0 & & 0 \\ & & \ddots & \ddots & \\ & & & 1 & 0 \\ & 0 & & & 1 & 0 \end{pmatrix}$$

$\xrightarrow{n} \quad \xrightarrow{n} \quad \xrightarrow{n}$

(在可換群, 左右正则表现一致)。

例 8 3 阶对称群的正则表示。

[解] 命  $a = (1\ 2)$ ,  $b = (1\ 3)$ , 那末  $\mathfrak{S}_3 = \{e, a, b, ab, ba, aba\}$ 。

左 群 表

$a^{-1}$	$b^{-1}$	$(ab)^{-1}$	$(ba)^{-1}$	$(aba)^{-1}$
$\parallel$	$\parallel$	$\parallel$	$\parallel$	$\parallel$
$e$	$a$	$b$	$ba$	$ab$
$a$	$e$	$ab$	$a^{-1}b$	$b$
$b$	$ba$	$e$	$a$	$aba$
$ab$	$a^{-1}ba$	$a$	$e$	$ba$
$ba$	$b$	$aba$	$ab$	$e$
$aba$	$ab$	$ba$	$b$	$a$

右 群 表

$a^{-1}$	$b^{-1}$	$(ab)^{-1}$	$(ba)^{-1}$	$(aba)^{-1}$
$\parallel$	$\parallel$	$\parallel$	$\parallel$	$\parallel$
$e$	$a$	$b$	$ba$	$ab$
$a$	$e$	$ba$	$b$	$aba$
$b$	$ab$	$e$	$a^{-1}ba$	$a$
$ab$	$b$	$a^{-1}ba$	$e$	$ba$
$ba$	$aba$	$a$	$ab$	$e$
$a^{-1}ba$	$ba$	$ab$	$a$	$b$

① 因为表示排列  $\pi = \begin{pmatrix} e & a & b & \dots & x & \dots \\ a^{-1} & e & a^{-1}b & \dots & a^{-1}x & \dots \end{pmatrix}$  的矩陣是分別以  $e, a, b, \dots, x, \dots$  为行数,  $a^{-1}, e, a^{-1}b, \dots, a^{-1}x, \dots$  为列数的元是 1 其他元为 0 的矩陣。今假定  $a^{-1}x = y$ , 那末在  $x$  行  $y$  列的元就应该换成 1, 但当  $a^{-1}x = y$  时,  $xy^{-1} = a$ , 反之, 假如  $xy^{-1} = a$ , 那末  $a^{-1}x = y$ , 这就是說把  $a^{-1}x$  换为 1 与把  $xy^{-1}$  换为 1 是一回事。所以在 (a) 中命  $a$  所在的地方为 1, 其他为 0 所得的矩陣就是表示排列的矩陣。——譯者注

左正则表现(依顺序表示  $e, a, b, ab, ba, aba$ )

$$\begin{pmatrix} 1 & & & & & \\ & 1 & & & & \\ & & 1 & & & \\ & & & 1 & & \\ & & & & 1 & \\ & & & & & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 & & & & \\ & & & & & \\ & & 1 & & & \\ & & & 1 & & \\ & & & & 1 & \\ & & & & & 1 \end{pmatrix}, \begin{pmatrix} & & 1 & & & \\ & & & & 1 & \\ 1 & & & & & \\ & & & & & 1 \\ & 1 & & & & \\ & & 1 & & & \end{pmatrix}, \begin{pmatrix} & & & 1 & & \\ & & 1 & & & \\ & & & & & \\ 1 & & & & & \\ & & & & 1 & \\ & 1 & & & & \end{pmatrix},$$

$$\begin{pmatrix} & & & 1 & & \\ & & & & 1 & \\ & 1 & & & & \\ & & & & & 1 \\ & & & 1 & & \\ 1 & & & & & \end{pmatrix}, \begin{pmatrix} & & & & 1 & \\ & & & & & 1 \\ & & & 1 & & \\ & & & & 1 & \\ & 1 & & & & \\ & & 1 & & & \end{pmatrix}$$

(空白部分都是 0)。

右正则表现(同上)

$$\begin{pmatrix} 1 & & & & & \\ & 1 & & & & \\ & & 1 & & & \\ & & & 1 & & \\ & & & & 1 & \\ & & & & & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 & & & & \\ & & & & & \\ & & 1 & & & \\ & & & 1 & & \\ & & & & 1 & \\ & & & & & 1 \end{pmatrix}, \begin{pmatrix} & & 1 & & & \\ & & & & 1 & \\ 1 & & & & & \\ & & & & & 1 \\ & 1 & & & & \\ & & 1 & & & \end{pmatrix}, \begin{pmatrix} & & & 1 & & \\ & & 1 & & & \\ & & & & & \\ 1 & & & & & \\ & & & & 1 & \\ & 1 & & & & \end{pmatrix},$$

$$\begin{pmatrix} & & & 1 & & \\ & & & & 1 & \\ & 1 & & & & \\ & & & & & 1 \\ & & & 1 & & \\ 1 & & & & & \end{pmatrix}, \begin{pmatrix} & & & & 1 & \\ & & & & & 1 \\ & & & 1 & & \\ & & & & 1 & \\ & 1 & & & & \\ & & 1 & & & \end{pmatrix}.$$

**例 9** 上面的  $\begin{pmatrix} x \\ a^{-1}x \end{pmatrix}$  或  $\begin{pmatrix} x \\ xa \end{pmatrix}$  可以看成为  $G$  中  $n$  个元的置换(133 页), 当  $a$  在  $G$  中变动时, 这种置换成为与  $G$  同构的群。一般自群  $G$  到有限集合  $S$  的对称群  $\mathfrak{S}(S)$  中的同态映射, 叫做  $G$  由置换群的表现。左右正则表现是由置换群表现的例。假定  $H$  是  $G$  的任意子群, 如果, 命  $G$  中  $H$  的剩余类的集合  $\{xH; x \in G\} = S$ , 那末, 对于  $a \in G$ , 使  $\begin{pmatrix} xH \\ axH \end{pmatrix} \in \mathfrak{S}(S)$  对应, 又得到  $G$  由置换群的表现。又关于  $H$  的右剩余类的集合  $\{Hx; x \in G\}$ , 对于  $a$  使与  $\begin{pmatrix} Hx \\ Hxa^{-1} \end{pmatrix}$  对应也得到  $G$  由置换群的表现(当  $H = \{e\}$  时, 就得到左右正则表现)。可以证明  $G$  由置换群的表现都能够象这样得到<sup>①</sup>。例如, 假定

<sup>①</sup> 参看 H. Zassenhaus: Lehrbuch der Gruppentheorie, p. 33, §2. — 译者注

$G = \mathfrak{S}_3$ , 如果  $H = G$ , 当然是恒等表现; 如果  $H = \{1, (1\ 2\ 3), (1\ 3\ 2)\}$ , 那就是交代表现; 如果  $H = \{1, (1\ 2)\}$ , 就得到下面的表现:

$$\begin{aligned} e &\leftrightarrow \begin{pmatrix} II & H_1 & H_2 \\ H & H_1 & H_2 \end{pmatrix} = E, \quad a \leftrightarrow (H_1 \ H_2), \quad b \leftrightarrow (II \ II_1), \\ ab &\leftrightarrow (H \ II_2 \ H_1), \quad ba \leftrightarrow (H \ H_1 \ II_2), \quad aba \leftrightarrow (H \ II_2), \\ \text{这里} \quad II_1 &= bII = \{b, ba\}, \quad H_2 = abII = \{ab, aba\}. \end{aligned}$$

### § 30 内自同构与伴随表现

假定对于群  $G$  中元  $x$ , 使  $axa^{-1}$  (但  $a \in G$ ) 与之对应(自  $G$  到  $G$  的)的映射用  $\varphi_a$  表示, 显然

$$\varphi_a(x) \varphi_a(y)^{-1} = \varphi_a(xy^{-1}), \quad (30.1)$$

$$\left. \begin{aligned} \varphi_e(x) &= x, \\ \varphi_a \circ \varphi_b(x) &= \varphi_{ab}(x), \\ \varphi_{a^{-1}}(x) &= \varphi_a^{-1}(x). \end{aligned} \right\} \quad (30.2)$$

其中(30.1)表示  $\varphi_a$  是自  $G$  到它自身的同构映射, 即  $G$  的自同构。 $G$  的自同构全体成为  $G$  的自同构群(146 页, 例 4)。表为  $\mathfrak{U}(G)$ 。(30.2) 表示  $\{\varphi_a; a \in G\} = \mathfrak{U}_0(G)$  成为  $\mathfrak{U}(G)$  的子群, 叫做  $G$  的**内自同构群**, 它的元  $\varphi_a$  叫做  $G$  的**内自同构**。(与此相应,  $\mathfrak{U}(G) = \mathfrak{U}_0(G)$  中元叫做  $G$  的**外自同构**。)

假如对于  $x, y \in G$ , 存在使  $\varphi_a(x) = y$  成立的  $a \in G$  时, 写成  $x \sim y$ , 显然  $\sim$  是等价关系。当  $x \sim y$  时,  $x, y$  叫做属于在  $G$  的**同类(或共轭类)**。 $\{y: x \sim y\}$  叫做  $x$  的类, 用  $C(x)$  表示。

**例 1** 单位元  $e$  的类只由一个  $e$  构成。可换群中各元形成只含它自身的类。

**命题 6**  $C(x)$  只由一个元  $\{x\}$  构成的这样的  $G$  中元  $x$  是与  $G$  中所有元可换。又它的逆也成立。这种元全体的集合成为  $G$  的可换正规子群(这个正规子群叫做  $G$  的**中心**)。

**证明**  $C(x) = \{x\}$  与对于任意  $a \in G$ ,  $axa^{-1} = x$  即  $ax = xa$  等

价。又这种元构成  $G$  的子群  $Z$  由下面关系容易明白:

- (i) 对于任意  $a \in G$ ,  $ae = ea$ .
- (ii) 假如  $ax = xa$ ,  $ay = ya$ , 那末  $axy = xay = xy a$ .
- (iii) 假如  $ax = xa$ , 那末  $xa^{-1} = a^{-1}x$ .

因为  $Z$  中元与  $G$  中所有元可换, 所以  $Z$  显然是  $G$  的可换正规子群。

**例 2**  $G = \mathfrak{S}_3$  的中心只由单位元  $e$  构成。把  $G$  用上面的意义来类别就得到

$$\{1\}, \{(1\ 2), (2\ 3), (3\ 1)\}, \{(1\ 2\ 3), (1\ 3\ 2)\}.$$

**例 3** 对称群的类别。

在上例 2 中, 已把  $\mathfrak{S}_3$  类别, 现在一般来考虑类别  $\mathfrak{S}_n$ .

$\mathfrak{S}_n$  中元  $\pi = \begin{pmatrix} 1 & 2 & \cdots & n \\ \nu_1 & \nu_2 & \cdots & \nu_n \end{pmatrix}$  能够表为不含共同文字的循环置换的乘积。譬如假定  $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 1 & 4 & 3 & 5 & 2 \end{pmatrix}$ , 那末  $\pi = (1\ 6\ 2)(3\ 4)(5)$  (一般, 能够用关于  $n$  的数学归纳法证明), 这些循环置换显然是可换的,  $\pi$  象这样的“分解”, 除因子的顺序外是唯一确定的。假定这些循环置换的个数是  $k = k(\pi)$ , 次数 ( $r$  个文字的循环置换叫做**次数**  $r$ ) 分别是  $r_1(\pi), r_2(\pi), \dots, r_k(\pi)$  ( $r_1(\pi) \geq \dots \geq r_k(\pi)$ ), 那末

$$\pi \sim \pi' \Leftrightarrow k(\pi) = k(\pi'), r_1(\pi) = r_1(\pi'), \dots, r_k(\pi) = r_k(\pi'). \quad (30.3)$$

实际上, 假如  $\pi = \begin{pmatrix} 1 & \cdots & n \\ \nu_1 & \cdots & \nu_n \end{pmatrix}$ , 如果  $\pi \sim \pi'$ , 因为由 134 页例 2 能够表  $\pi' = \begin{pmatrix} \mu_1 & \cdots & \mu_n \\ \mu_{\nu_1} & \cdots & \mu_{\nu_n} \end{pmatrix}$ , 所以在  $\pi$  的分解中命  $\mu_i$  代替  $i$ , 就得到  $\pi'$  的分解。反之, 假如  $k(\pi) = k(\pi'), r_j(\pi) = r_j(\pi'), j = 1, \dots, k$ , 如果在  $\pi, \pi'$  分解中对应位置的数字分别作为  $i, \mu_i$ , 命  $\pi = \begin{pmatrix} 1 & \cdots & n \\ \mu_1 & \cdots & \mu_n \end{pmatrix}$ , 那末  $\pi' = \pi \pi \pi^{-1}$ .

$I(\pi) = (r_1(\pi), \dots, r_k(\pi))$  叫做  $\pi$  的不变系, 由 (30.3),  $\pi$  的类由它的不变系决定。所以  $\mathfrak{S}_n$  的类的个数等于不定方程式

$$x_1 + x_2 + \cdots + x_n = n, \quad x_1 \geq x_2 \geq \cdots \geq x_n \geq 0$$

中整数解的个数。

假定  $i$  是  $1 \leq i \leq n$  的整数,  $r_1(\pi), \dots, r_k(\pi)$  中等于  $i$  的数的个数是

$\lambda_i(x)$ , 那末由

$$J(x) = (\lambda_1(x), \dots, \lambda_n(x))$$

能够决定  $I(x)$ , 所以  $x$  的类由  $J(x)$  确定。这时显然

$$\lambda_1(x) + 2\lambda_2(x) + \dots + n\lambda_n(x) = n.$$

又假如  $\lambda_1, \lambda_2, \dots, \lambda_n$  是满足  $\lambda_1 + 2\lambda_2 + \dots + n\lambda_n = n$  的非负整数, 那末满足  $J(x) = (\lambda_1, \lambda_2, \dots, \lambda_n)$  的  $x$  存在, 象这样的  $x$  的个数  $n(\lambda_1, \dots, \lambda_n)$  由

$$n(\lambda_1, \dots, \lambda_n) = \frac{n!}{\prod_{k=1}^n \lambda_k! k^{\lambda_k}}$$

给出。这是因为对于  $n$  个文字的任意排列, 由于引入如下的括弧

$$\begin{array}{ccccccc} (\nu_1) (\nu_2) \cdots (\nu_{\lambda_1}) (\nu_{\lambda_1+1} \nu_{\lambda_1+2}) \cdots (\nu_{\lambda_1+2\lambda_1-1} \nu_{\lambda_1+2\lambda_1}) \cdots \\ \longleftarrow \lambda_1 \text{ 个} \longrightarrow & \longleftarrow \lambda_2 \text{ 个} \longrightarrow & \longrightarrow & \longrightarrow \end{array}$$

能够得到属于这种不变系的  $x$ , 其中由于长相相同的循环置换的排列有  $\prod_{k=1}^n \lambda_k!$  个, 且由于在一个循环置换中把文字循环互换的排列  $\prod_{k=1}^n k^{\lambda_k}$  个都给出相同的置换。

5 次以下对称群的共轭类揭示如表:

群	类的記号	不变系 $I(C)$	$J(C)$	代 表 元	元数 $n(C)$
$\mathfrak{S}_2$	$C_1$	(1, 1)	(2, 0)	1	1
	$C_2$	(2)	(0, 1)	(1 2)	1
$\mathfrak{S}_3$	$C_1$	(1, 1, 1)	(3, 0, 0)	1	1
	$C_2$	(2, 1)	(1, 1, 0)	(1 2)	3
	$C_3$	(3)	(0, 0, 1)	(1 2 3)	2
$\mathfrak{S}_4$	$C_1$	(1, 1, 1, 1)	(4, 0, 0, 0)	1	1
	$C_2$	(2, 1, 1)	(2, 1, 0, 0)	(1 2)	6
	$C_3$	(2, 2)	(0, 2, 0, 0)	(1 2) (3 4)	3
	$C_4$	(3, 1)	(1, 0, 1, 0)	(1 2 3)	8
	$C_5$	(4)	(0, 0, 0, 1)	(1 2 3 4)	6
$\mathfrak{S}_5$	$C_1$	(1, 1, 1, 1, 1)	(5, 0, 0, 0, 0)	1	1
	$C_2$	(2, 1, 1, 1)	(3, 1, 0, 0, 0)	(1 2)	10
	$C_3$	(2, 2, 1)	(1, 2, 0, 0, 0)	(1 2) (3 4)	15
	$C_4$	(3, 1, 1)	(2, 0, 1, 0, 0)	(1 2 3)	20
	$C_5$	(3, 2)	(0, 1, 1, 0, 0)	(1 2 3) (4 5)	20
	$C_6$	(4, 1)	(1, 0, 0, 1, 0)	(1 2 3 4)	30
	$C_7$	(5)	(0, 0, 0, 0, 1)	(1 2 3 4 5)	24

**命题 7**  $G$  中属于同一共轭类中元的个数等于  $G$  的阶的约数。

这命题的证明要引用“正规化群”的概念。假定  $M$  是  $G$  的任意子集合, 容易得知  $G$  中与  $M$  (作为全体) 可换的元全体的集合  $\{x; xM = Mx\}$  成为  $G$  的子群。它叫做 (在  $G$ )  $M$  的正规化群 (normalizer), 用  $N(M)$  表示 (假如  $M$  是  $G$  的正规子群, 那末  $G = N(M)$ ), 又假如  $M$  是  $G$  的任意子群, 那末  $M$  是  $N(M)$  的正规子群。因此有这名称)。

显然因为

$$xMx^{-1} = M \Leftrightarrow xM = Mx \Leftrightarrow x \in N(M),$$

更一般

$$\begin{aligned} xMx^{-1} = yMy^{-1} &\Leftrightarrow y^{-1}xM = My^{-1}x \\ &\Leftrightarrow y^{-1}x \in N(M) \Leftrightarrow xN(M) = yN(M), \end{aligned}$$

所以它与  $x, y$  属于关于  $\text{mod } N(M)$  的同一左剩余类等价。于是当  $x$  取  $G$  中任意元时,  $xMx^{-1}$  形状的  $G$  子集合的个数等于  $G$  中关于  $\text{mod } N(M)$  的左剩余类的个数, 即  $(G:N(M))$ , 它当然是  $(G:\{e\}) = n$  的约数。

特别, 考虑  $M$  只由一个  $G$  元  $a$  构成的情形:  $M = \{a\}$ 。这时  $xMx^{-1}$  也只由一个元  $axa^{-1}$  构成。于是当  $x$  取  $G$  中元时, 能够成为  $axa^{-1}$  的不外是与  $a$  共轭的元。它的个数因为是  $M = \{a\}$  的正规化群  $N(a)$  的指数, 所以是  $n$  的约数 (命题 7 证毕)。

把群代数  $A(G)$  作为表现空间, 能够作成象下面这样异于正则表现的表现。即假如对于  $A(G)$  的基底  $f_e \in A(G)$ , 使  $f_{\tau(a)(e)}$  对应的  $\mathfrak{L}(A(G))$  中元作为  $\tau(a)$ , 来考虑对于  $a \in G$  使  $\tau(a) \in GL(A(G))$  的对应  $\tau: G \rightarrow GL(A(G))$ 。显然  $\tau$  成为  $G$  的表现, 它叫做  $G$  的伴随表现。伴随表现的核  $\tau^{-1}(e)$  是  $G$  的中心。

**例 4**  $\mathfrak{S}(\{1, 2, 3\})$  的伴随表现



$f_x$	$e$	$a$	$b$	$ab$	$ba$	$aba$
$\tau(e)f_x$	$e$	$a$	$b$	$ab$	$ba$	$aba$
$\tau(a)f_x$	$e$	$a$	$aba$	$ba$	$ab$	$b$
$\tau(b)f_x$	$e$	$aba$	$b$	$ba$	$ab$	$a$
$\tau(ab)f_x$	$e$	$b$	$aba$	$ab$	$ba$	$a$
$\tau(ba)f_x$	$e$	$aba$	$a$	$ab$	$ba$	$b$
$\tau(aba)f_x$	$e$	$b$	$a$	$ba$	$ab$	$aba$

$e, a, b, ab, ba, aba$  分别用下面的矩阵表示

$$\begin{pmatrix} 1 & & & & & \\ & 1 & & & & \\ & & 1 & & & \\ & & & 1 & & \\ & & & & 1 & \\ & & & & & 1 \end{pmatrix}, \begin{pmatrix} 1 & & & & & \\ & 1 & & & & \\ & & & & 1 & \\ & & & & & 1 \\ & & & 1 & & \\ & & & & 1 & \end{pmatrix}, \begin{pmatrix} 1 & & & & & \\ & 1 & & & & \\ & & & 1 & & \\ & & & & 1 & \\ & & & & & 1 \\ & & 1 & & & \end{pmatrix}, \begin{pmatrix} 1 & & & & & \\ & 1 & & & & \\ & & & & 1 & \\ & & & & & 1 \\ & & 1 & & & \\ & & & 1 & & \end{pmatrix}, \\
\begin{pmatrix} 1 & & & & & \\ & 1 & & & & \\ & & & 1 & & \\ & & & & 1 & \\ & & 1 & & & \\ & & & 1 & & \end{pmatrix}, \begin{pmatrix} 1 & & & & & \\ & 1 & & & & \\ & & 1 & & & \\ & & & 1 & & \\ & & & & 1 & \\ & & & & & 1 \end{pmatrix}.$$

### § 31 直交关系

由 Schur 引理能够导出下面的基本定理。

**定理 11** 假定  $\rho_1, \rho_2$  是有限群  $G$  的两个既约表现,  $V_1, V_2$  分别是  $\rho_1, \rho_2$  的表现空间,  $\psi$  是自  $V_1$  到  $V_2$  的线性映射, 这时如果

$$\varphi = \sum_{a \in G} \rho_2(a) \circ \psi \circ \rho_1(a^{-1}), \quad (31.1)$$

那末  $\varphi$  成为自  $V_1$  到  $V_2$  的线性映射, 假如  $\rho_1 \not\sim \rho_2$ , 那末  $\varphi = 0$ . 又假如  $\rho_1 \sim \rho_2$ , 如果  $\dim V_1 = \dim V_2 = m$ ,  $G$  的阶  $= n$ , 把  $x \in V_1$  与  $\psi(x) \in V_2$ ,  $\rho_1(a)$  与  $\rho_2(a)$  同样看待, 那末  $\varphi = \frac{n}{m} S(\psi)$ .

这里  $S(\psi)$  的意义如下。假如取  $V_1$  的任意坐标系,  $\psi$  就能够

用矩阵表示。这矩阵的迹 (75 页例 3) 与坐标系的取法无关。因此这迹就用  $S(\psi)$  表示 (参照 76 页)。

**证明** 由 (31.1) 立即得到

$$\varphi \circ \rho_1(a) = \rho_2(a) \circ \varphi,$$

所以, 假如不是  $\rho_1 \sim \rho_2$ , 由 Schur 引理的系,  $\varphi = 0$ . 当  $\rho_1 \sim \rho_2$  时, 如果把  $x \in V_1$  与  $\psi(x) \in V_2$ ,  $\rho_1(a)$  与  $\rho_2(a)$  同样看待, 那末由定理 3 系 1,  $\varphi = \alpha \in C$ . 取这式两边的迹, 即得

$$m\alpha = S(\varphi) = \sum S(\rho_1(a) \circ \psi \circ \rho_1(a^{-1})) = \sum S(\psi) = nS(\psi).$$

所以 
$$\alpha = \frac{n}{m} S(\psi). \quad (\text{证毕})$$

于是把  $\varphi$  特殊化, 即得下面的定理。

**定理 12** 对于有限群  $G$  的两个既约矩阵表现  $A(x) = (a_{ij}(x))$ ,  $B(x) = (b_{kl}(x))$ , 下面的关系成立:

如果不是  $A \sim B$ ,

$$\sum_{x \in G} a_{ij}(x) b_{kl}(x^{-1}) = 0, \quad (31.2)$$

如果  $A \sim B$ , 它的次数是  $m$ ,  $G$  的阶是  $n$ ,

$$\sum_{x \in G} a_{ij}(x) b_{kl}(x^{-1}) = \frac{n}{m} \delta_{jk} \delta_{il}. \quad (31.3)$$

**证明** 假定  $A, B$  分别是  $G$  的既约表现  $\rho_1, \rho_2$  的矩阵表现, 它们的表现空间是  $V_1, V_2$ . 如果在  $V_1, V_2$  分别取适当的坐标系,  $\rho_1(x), \rho_2(x)$  能够分别用矩阵  $A(x), B(x)$  表示。现在, 以这坐标系作为定理 11 中的  $\psi$ , 取关于这坐标系, 用 § 8 命题 10 证明中 (39 页) 的矩阵  $E'_{jk}$  所表示的线性映射。然后把定理 11 的结果改写, 就立即得到 (31.2), (31.3)。

**系 1** 假定把  $a_{ij}, b_{kl}$  考虑为对于“变数”  $x \in G$ , 值取  $C$  中  $a_{ij}(x), b_{kl}(x)$  数的  $A(G)$  中元, 那末在  $A(G)$  中, 乘法 (§ 29) 的意义如下:

如果不是  $A \sim B$ ,

$$b_{kl} \cdot a_{ij} = 0, \quad (31.4) \textcircled{1}$$

一般

$$a_{kl} \cdot a_{ij} = \frac{n}{m} \delta_{li} a_{kj}. \quad (31.5) \textcircled{1}$$

(31.2), (31.3), (31.4), (31.5) 叫做既約表現的直交关系。

又对于  $f, g \in A(G)$ , 如果

$$(f, g) = \frac{1}{n} \sum_{x \in G} f(x) \overline{g(x)}, \quad (31.6)$$

那末  $(f, g)$  显然满足 § 17 中  $U1 \sim 5$ , 因此  $A(G)$  成为具有这种“内积”的内空间。

由 § 27 定理 8, 有限群  $G$  的任意表现  $\rho$ , 与西表现等价。因此适当地取表现空间  $V$  的基底它能够用西矩阵  $P(a) = (p_{ij}(a))$  表示。因为  $P(a)$  是西矩阵, 所以

$$\overline{P(a)} = P(a^{-1}).$$

① 关于 (31.4), (31.5) 两式, 我们只要证明 (31.5), 至于 (31.4) 可以同样推出。由  $A(G)$  的乘法定义得

$$\begin{aligned} a_{kl} &= a_{ij} = \sum_{x \in G} \left[ \sum_{y \in G} a_{kl}(xy^{-1}) a_{ij}(y) \right] f_x, \\ a_{kj} &= \sum_{x \in G} a_{kj}(x) f_x. \end{aligned}$$

因此只须证明

$$\sum_{y \in G} a_{kl}(xy^{-1}) a_{ij}(y) = \frac{n}{m} \delta_{li} a_{kj}(x) \quad (1)$$

即可, 为此我们在

$$D = \sum_{y \in G} A(y^{-1}) C A(y)$$

中假定  $C$  是只有  $l$  行  $i$  列的元为 1 其余的元都等于零的矩阵, 那末

$$\frac{n}{m} \delta_{li} \cdot E = \sum_{y \in G} A(y^{-1}) C A(y)$$

成立(把定理 12 的证明用矩阵表示即得)。

由所取的  $C$  将上式用矩阵元即得

$$\frac{n}{m} \delta_{li} (a_{kj}(x)) = \sum_{y \in G} a_{kl}(xy^{-1}) a_{ij}(y).$$

比较两边矩阵的元素即得 (1) 式。——译者注

于是  $p_{ij}: a \rightarrow p_{ij}(a)$  能够看成为  $A(G)$  中元。如果引用 (31.6) 的内积 (由于  ${}^t\overline{P(a)} = P(a^{-1})$ ) 上系能够改写如下

**系 2** 假定  $\rho_1, \rho_2$  是有限群  $G$  的两个既约表现,  $P_1 = (p_{ij}^{(1)})$  及  $P_2 = (p_{kl}^{(2)})$  是它们用酉矩阵的表现, 那末在 (31.6) 内积的意义下,

$$(p_{ij}^{(1)}, p_{kl}^{(2)}) = \begin{cases} 0, & \rho_1 \not\sim \rho_2, \\ \frac{1}{m} \delta_{ik} \delta_{jl}, & \rho_1 \sim \rho_2 \text{ (} m \text{ 是 } \rho_1, \rho_2 \text{ 的级数)}. \end{cases}$$

由这系更导出下面的重要事实。

**定理 13** (Burnside) 假定  $P = (p_{ij})$  是有限群  $G$  由  $m$  级矩阵的既约表现, 那末  $m^2$  个  $A(G)$  中元  $p_{ij}$  在  $C$  上是线性无关的。又假如  $Q = (q_{kl})$  是  $G$  的  $m'$  级既约矩阵表现且与  $P$  不等价, 那末  $m^2 + m'^2$  个  $A(G)$  中元  $p_{ij}, q_{kl}$  在  $C$  上是线性无关的。

**证明** 因为  $P(a)$  能够用 (与  $a$  无关系)  $m$  级正则矩阵  $T$  变换为酉矩阵  $P_0(a): T^{-1}P(a)T = P_0(a)$ , 如果  $P_0(a) = (p_{ij}^0(a))$ , 那末  $p_{ij}^0(a)$  成为  $p_{ij}(a)$ ,  $i, j = 1, \dots, m$  的线性组合。反之, 因为  $P(a) = TP_0(a)T^{-1}$ , 所以  $p_{ij}(a)$  成为  $p_{ij}^0(a)$ ,  $i, j = 1, \dots, m$  的线性组合。因此  $[p_{11}, p_{12}, \dots, p_{mm}] = [p_{11}^0, p_{12}^0, \dots, p_{mm}^0]$ 。所谓  $p_{11}, p_{12}, \dots, p_{mm}$  是线性无关, 意味着  $A(G)$  的子空间  $[p_{11}, p_{12}, \dots, p_{mm}]$  的维数是  $m^2$ 。因为此时说成  $\dim [p_{11}^0, p_{12}^0, \dots, p_{mm}^0] = m^2$  也可, 所以自开始即假令  $P$  是酉表现并不失一般性。这时由前定理的系 2,

$$(p_{ij}, p_{kl}) = \frac{1}{m} \delta_{ik} \delta_{jl}$$

即  $p_{11}, p_{12}, \dots, p_{mm}$  成为在  $A(G)$  的直交系。因此由 96 页命题 48 的系 1, 它们是线性无关的。后半段也能够同样证明。

## § 32 特征标

假定  $\rho$  是有限群  $G$  的  $m$  级表现, 对于  $a \in G$ , 使  $\rho(a)$  的迹

(76頁)  $S(\rho(a))$  对应的函数用  $\chi_\rho(a)$  表示。 $\chi_\rho$  能够看成为  $A(G)$  中元,  $\chi_\rho$  叫做  $\rho$  的特征标。

例1  $\chi_\rho(e) = (\rho \text{ 的級数})$ 。

例2 正则表现  $\rho$  的特征标。如果  $a \neq e$ , 那末  $\chi_\rho(a) = 0$ 。

[解] 在左正则表现, 表示  $\rho(a)$  的矩阵是表示排列  $\begin{pmatrix} x \\ a^{-1}x \end{pmatrix}$  的矩阵, 假如  $a \neq e$ , 那末  $x \neq a^{-1}x$ 。因此, 这矩阵主对角线上元素都是 0。所以  $\chi_\rho(a) = 0$ 。关于右正则表现也是同样。

特别, 假如  $\rho$  是既约, 那末  $\chi_\rho$  叫做单纯特征标。由定理 8 系, 有限群  $G$  的任意表现  $\rho$ , 能够表为既约表现  $\rho_1, \dots, \rho_r$  的直和  $\rho_1 \oplus \dots \oplus \rho_r$ 。这时由 §14 命题 39, 立即得到

$$\chi_\rho = \chi_{\rho_1} + \dots + \chi_{\rho_r}.$$

于是得到下面的命题。

**命题 8** 有限群的任意表现的特征标能够表为单纯特征标的和。

例3 在可换群, 因为既约表现是 1 級的, 所以它的特征标与表现自身一致。即假如  $\chi = \chi_\rho$  是可换群  $G$  的单纯特征标, 那末对于  $x, y \in G$  有  $\chi(xy) = \rho(xy)$  (詳細点說即意味着  $\chi(x)e = \rho(x)$ )。又  $\chi(xy^{-1}) = \chi(x)\chi(y)^{-1}$ 。更假如  $G$  是有限群, 那末  $x$  的阶  $m$  有限 ( $G$  的阶  $n$  的約数), 因为  $x^m = e$ , 所以  $\chi(x)$  是 1 的  $m$  乘根 (因此是  $n$  乘根)。

例4 一般, 假定  $G$  是有限群 (阶  $n$ ),  $x \in G$ ,  $m$  是  $x$  的阶, 如果  $\rho$  是  $G$  的表现,  $P$  是它的矩阵表现, 那末  $\chi_\rho(x) = S(P(x))$ 。但  $x^m = e$ , 所以  $(P(x))^m = E$ , 因此矩阵  $P(x)$  滿足方程  $X^m = E$ , 于是  $P(x)$  的特征值成为 1 的  $m$  乘根 (因而是  $n$  乘根)。(假如  $(r, r)$  型矩阵  $X$  的特征值是  $\alpha_1, \dots, \alpha_r$ , 如果改成 Jordan 标准形来看就容易得知,  $X^m$  的特征值是  $\alpha_1^m, \dots, \alpha_r^m$ 。因此, 如果  $X^m = E$ , 那末  $\alpha_i^m = 1$ 。) 所以  $\chi_\rho(x)$  所取的值都是 1 的  $n$  乘根的和。

在上面曾引用 76 頁命题 38 的系及命题 39 的

$$(i) \quad S(TFT^{-1}) = S(F),$$

$$(ii) \quad S(F_1 \oplus F_2) = S(F_1) + S(F_2)$$

作为迹的性质, 再又有

(iii) 当  $F_1 \in \mathfrak{M}(m_1, \mathbb{C})$ ,  $F_2 \in \mathfrak{M}(m_2, \mathbb{C})$  时,

$$S(F_1 \otimes F_2) = S(F_1) \cdot S(F_2).$$

它又能够象下面那样表示:

假如  $F_1 = (a_{ij})$ ,  $F_2 = (b_{kl})$ , 那末

$$S(F_1 \otimes F_2) = \sum_{i,k} a_{ii} b_{kk} = S(F_1) \cdot S(F_2).$$

引用这些性质立即得到下面的命题:

**命题 9** (i) 假定  $\rho_1 \sim \rho_2$ , 那末  $\chi_{\rho_1} = \chi_{\rho_2}$ .

(ii)  $\chi_\rho(a) = \chi_\rho(bab^{-1})$ ,  $a, b \in G$ .

(iii)  $\chi_{\rho_1 \oplus \rho_2}(a) = \chi_{\rho_1}(a) + \chi_{\rho_2}(a)$ .

(iv)  $\chi_{\rho_1 \otimes \rho_2}(a) = \chi_{\rho_1}(a) \chi_{\rho_2}(a)$ .

更由定理 12 的系 2, 得

**定理 14** 假定  $\rho_1, \rho_2$  是既约表现, 那末

$$(\chi_{\rho_1}, \chi_{\rho_2}) = \begin{cases} 0, & \rho_1 \not\sim \rho_2, \\ 1, & \rho_1 \sim \rho_2. \end{cases}$$

它叫做单纯特征标的直交关系。

由这与前节定理 13 同样得到下面的系。

**系 1** 假定  $\rho_1, \dots, \rho_r$  是有限群  $G$  不等价的既约表现, 那末单纯特征标  $\chi_{\rho_1}, \dots, \chi_{\rho_r}$  在  $\mathbb{C}$  上是线性无关。 (系 1 毕)

因为  $\chi_{\rho_i}$  都是  $A(G)$  中元,  $A(G)$  是  $(\mathbb{C}$  上)  $n$  维向量空间, 于是更得到下面的系。

**系 2** 阶为  $n$  的有限群的不等价既约表现的个数不大于  $n$  (参照后面的定理 21)。

象上面那样,  $G$  的任意表现  $\rho$ , 能够由既约表现  $\rho_1, \dots, \rho_r$  用直和

$$\rho = \rho_1 \oplus \dots \oplus \rho_r$$

的形状表示, 但是这时在  $\rho_1, \dots, \rho_r$  中也許有等价的, 假如把等价的分别集中, 命

$$\rho = m_1 \rho_1 \oplus \cdots \oplus m_k \rho_k \quad (m_i \text{ 是自然数}),$$

其中  $\rho_1, \dots, \rho_k$  沒有等价的, 那末  $m_i$  叫做  $\rho_i$  在  $\rho$  的重复度, 用  $(\rho: \rho_i)$  表示。

由上式立即得到

$$\chi_\rho = m_1 \chi_{\rho_1} + \cdots + m_k \chi_{\rho_k},$$

由定理 14 更得到下面的命题。

**命题 10**  $(\rho: \rho_i) = (\chi_\rho, \chi_{\rho_i})$ 。

下面的事实大都是定理 14 的系, 因为是特征标的重要性质, 所以特作为定理提出。

**定理 15** 有限群  $G$  的两个表现  $\rho, \sigma$  成为等价, 必要且只要  $\chi_\rho = \chi_\sigma$ 。

**証明**  $\rho \sim \sigma \Rightarrow \chi_\rho = \chi_\sigma$  已經在命题 9(i) 中示明。反之, 假如  $\chi_\rho = \chi_\sigma$ , 由上命题 10, 对于  $G$  的任意既約表现  $\rho_i$ ,  $(\rho: \rho_i) = (\sigma: \rho_i)$ , 所以  $\rho \sim (\rho: \rho_1) \rho_1 \oplus \cdots \oplus (\rho: \rho_k) \rho_k = (\sigma: \rho_1) \rho_1 \oplus \cdots \oplus (\sigma: \rho_k) \rho_k \sim \sigma$ 。  
(証毕)

由定理 14 更立即得到下面的定理。

**定理 16** 假定  $\rho_1, \dots, \rho_r$  是既約表现,  $\rho = m_1 \rho_1 \oplus \cdots \oplus m_r \rho_r$ , 那末  $(\chi_\rho, \chi_\rho) = m_1^2 + \cdots + m_r^2$ 。

**系 1**  $\rho$  是既約表现的必要充分条件是  $(\chi_\rho, \chi_\rho) = 1$ 。

由这最后的系,  $\rho$  是否是既約表现可以简单地只从特征标  $\chi_\rho$  来判別。

**系 2** 在有限群  $G$  的两个既約表现  $\rho_1, \rho_2$  中, 如果  $\rho_2$  是 1 級表现, 那末張量积表现  $\rho = \rho_1 \otimes \rho_2$  也是既約的。

$$\begin{aligned} \text{証明} \quad (\chi_\rho, \chi_\rho) &= \frac{1}{n} \sum_{a \in G} \chi_\rho(a) \overline{\chi_\rho(a)} \\ &= \frac{1}{n} \sum_{a \in G} \chi_{\rho_1}(a) \chi_{\rho_2}(a) \overline{\chi_{\rho_1}(a) \chi_{\rho_2}(a)}. \end{aligned}$$

这里因为  $\rho_2$  是 1 级既约表现, 所以  $\chi_{\rho_2}(a)$  是 1 的  $n$  乘根。因此

$$\chi_{\rho_2}(a) \overline{\chi_{\rho_2}(a)} = 1,$$

所以  $(\chi_\rho, \chi_\rho) = \frac{1}{n} \sum_{a \in G} \chi_{\rho_1}(a) \overline{\chi_{\rho_1}(a)} = (\chi_{\rho_1}, \chi_{\rho_1}) = 1.$

**例 5** 假定  $\rho$  是有限群  $G$  的  $d$  级任意 (不一定是既约) 表现, 如果  $\chi_\rho = \chi$ , 那末对于  $a \in G$ ,

$$(1) \chi(a^{-1}) = \overline{\chi(a)},$$

$$(2) |\chi(a)| \leq d,$$

$$(3) \text{ 假如 } \chi(a) = d, \text{ 那末, 对于任意 } x \in G \text{ 有 } \rho(x)\rho(a) = \rho(a)\rho(x).$$

[解] 假如  $\rho \sim \rho'$  那末  $\chi_\rho = \chi_{\rho'}$ . 因为有与  $\rho$  等价的酉表现, 所以  $\rho$  开始作为酉的并不失一般性。假定  $a \rightarrow P(a) = (p_{ij}(a))$  是  $\rho$  由酉矩阵的表现, 那末  $\chi(a) = \sum_{i=1}^d p_{ii}(a)$ . 因为  $P(a)$  是酉的, 所以

$$(1) P(a^{-1}) = (P(a))^{-1} = {}^t \overline{P(a)}. \text{ 因此 } \chi(a^{-1}) = \sum_{i=1}^d \overline{p_{ii}(a)} = \overline{\chi(a)},$$

$$(2) {}^t P(a) P(a) = E_d. \text{ 因此 } \sum_{j=1}^d |p_{ij}(a)|^2 = 1, |p_{ii}(a)| \leq 1, \text{ 于是 } |\chi(a)| \leq d.$$

(3)  $\chi(a) = d$  只有在  $p_{ii}(a) = 1, i = 1, \dots, d$  即  $P(a) = E_d$  时成立。这时, 对于任意  $x \in G, P(x)P(a) = P(a)P(x)$ . 因此  $\rho(x)\rho(a) = \rho(a)\rho(x)$ .

**例 6** 假定在  $G, a \sim a^{-1}$  ( $a$  与  $a^{-1}$  属于同一共轭类), 那末  $\chi(a) \in \mathbb{R}$ . 对于所有  $a \in G$ , 如果  $a \sim a^{-1}$ , 那末特征标所取的值都是实数。特别  $\mathfrak{S}_n$  的特征标都取实数值①。

[解] 由例 5(1) 显然。

**注意** 在后面将证明 (§ 41)  $\mathfrak{S}_n$  的特征标实际是有理整数。

### § 33 群代数 $A(G)$ 的构造

在上定理 14 的系 2 中已示明有限群  $G$  不相互等价的既约表

① 因为  $s \sim s^{-1}$ , 这是由于可以假定  $s$  是循环置换 (不然可以把  $s$  表为含不同文字的循环置换的乘积),  $s$  与  $s^{-1}$  具有相同的循环次数, 而两置换为共轭的必要充分条件是它们有共同的循环次数, 所以  $s \sim s^{-1}$ . 实际上, 假如  $s = (s_1 s_2 \dots s_k), t = (t_1 t_2 \dots t_k)$ ,

命  $p = \begin{pmatrix} s_1 & s_2 & \dots & s_k \\ t_1 & t_2 & \dots & t_k \end{pmatrix}$ , 那末  $p^{-1}p = t$ . ——译者注



現的个数是有限的。假定这数是  $q(G) = q$ ,  $\rho_1, \dots, \rho_q$  是自各既約表現类各取一个的既約表現, 即既約表現的“代表系”。这时有下面的重要定理成立。

**定理 17** 假定  $\rho$  是有限群  $G$  的正則表現,  $\rho_1, \dots, \rho_l$  是  $G$  的既約表現的代表系, 如果  $\rho_i$  的級数是  $d_i$ , 那末  $(\rho: \rho_i) = d_i$ .

**証明** 假定  $\rho = m_1 \rho_1 \oplus \dots \oplus m_q \rho_q$  来証明  $m_i = d_i$  即可。由命题 10,  $m_i = (\chi_\rho, \chi_{\rho_i}) = \frac{1}{n} \sum_{x \in G} \chi_\rho(x) \overline{\chi_{\rho_i}(x)}$  ( $n$  是  $G$  的阶)。但由 § 32 例 1, 例 2,  $\chi_\rho(e) = n$ ,  $\chi_{\rho_i}(e) = d_i$ , 假如  $x \neq e$ , 那末  $\chi_\rho(x) = 0$ . 所以

$$m_i = \frac{1}{n} \cdot n \cdot d_i = d_i. \quad (\text{証毕})$$

下面两个系是重要的。

**系 1**  $n = d_1^2 + \dots + d_q^2$ .

**証明** 由  $n = \chi_\rho(e) = d_1 \chi_{\rho_1}(e) + \dots + d_q \chi_{\rho_q}(e)$ , 自明。

**系 2** 有限群的所有既約表現是正則表現的子表現。

**例 1**  $G = \mathfrak{S}_3$  的既約表現已知有恒等表現  $\rho_1$ , 交代表現  $\rho_2$ , 2 級表現  $\rho_3$  三个。因为  $G$  的阶是 6, 而  $6 = 1^2 + 1^2 + 2^2$ , 所以  $G$  的既約表現与  $\rho_1, \rho_2, \rho_3$  中之一等价 (§ 27, 例 2, 但那里的記法—— $\rho_i$  的番号——与这里不同)。

假定有限群  $G$  的既約表現的代表系是  $\rho_1, \dots, \rho_q$ , 它們的級数分別是  $d_1, \dots, d_q$ , 如果  $\rho_i$  的矩陣表現  $x \rightarrow P_i(x) = (p_{ij}^{(i)}(x))$ , 那末  $p_{ij}^{(i)}(x) \in A(G)$ . 因为  $i, j$  是自 1 到  $d_i$  变动, 所以全部能够得到  $\sum_{i=1}^q d_i^2$  个  $A(G)$  中元。它們叫做由既約矩陣表現的代表系  $P_1, \dots, P_q$  所确定的基本函数系。

**定理 18** 基本函数系形成  $A(G)$  的基底。

**証明** 由 Burnside 定理, 基本函数系在  $\mathbb{C}$  上是綫性无关。并且它的个数  $\sum_{i=1}^q d_i^2$  由前面定理系 1 等于  $A(G)$  的維数  $n$ . 所以由 § 5 即得本定理。

**定理 19** 假定有限群  $G$  的既約表現的代表系  $\rho_1, \dots, \rho_q$  的級

数分别是  $d_1, \dots, d_q$ , 那末  $G$  的群代数  $A(G)$  与  $q$  个矩阵环的直和  $\mathfrak{M}(d_1, \mathbb{C}) \oplus \dots \oplus \mathfrak{M}(d_q, \mathbb{C})$  作为代数是同构。

**证明** 假定  $\rho_\nu$  的矩阵表现是  $P_\nu = (p_{ij}^{(\nu)})$ , 前定理已示明  $p_{ij}^{(\nu)}$ ,  $i, j = 1, \dots, d_\nu; \nu = 1, \dots, q$  构成  $A(G)$  的基底。但由定理 12 的系 1 中直交关系式, 命  $\frac{d_\nu}{n} p_{ij}^{(\nu)} = e_{ij}^{(\nu)}$ , 得

$$\begin{cases} e_{ij}^{(\nu)} \cdot e_{kl}^{(\mu)} = 0, & \nu \neq \mu, \\ e_{ij}^{(\nu)} \cdot e_{kl}^{(\nu)} = \delta_{jk} e_{il}^{(\nu)}. \end{cases} \quad (33.1)$$

这等  $e_{ij}^{(\nu)}$ ,  $i, j = 1, \dots, d_\nu; \nu = 1, \dots, q$  显然也构成  $A(G)$  的基底, 如果对于  $x = \sum_{i,j,\nu} \alpha_{ij}^{(\nu)} e_{ij}^{(\nu)} \in A(G)$ , 命

$$Q^{(\nu)}(x) = \begin{pmatrix} \alpha_{11}^{(\nu)} & \dots & \alpha_{1d_\nu}^{(\nu)} \\ \dots & \dots & \dots \\ \alpha_{d_\nu 1}^{(\nu)} & \dots & \alpha_{d_\nu d_\nu}^{(\nu)} \end{pmatrix},$$

$$Q(x) = Q^{(1)}(x) \oplus \dots \oplus Q^{(q)}(x),$$

那末  $x \rightarrow Q(x)$  显然给出自  $A(G)$  到  $\mathfrak{M}(d_1, \mathbb{C}) \oplus \dots \oplus \mathfrak{M}(d_q, \mathbb{C})$  上的同构表现。 (証毕)

在前面定义了群的中心 (§ 30), 对于代数  $A$  也能够象下面那样来定义它的中心。容易验证

$$C(A) = \{x; ax = xa, \forall a \in A\}$$

(与  $A$  中所有元可换的  $A$  中元的集合) 成为  $A$  的子代数,  $C(A)$  叫做代数  $A$  的**中心**。

**例 2**  $C(A_1 \oplus \dots \oplus A_k) = C(A_1) \oplus \dots \oplus C(A_k)$ 。

**定理 20** 有限群  $G$  的单纯特征标的全体形成代数  $A(G)$  的中心  $C(A(G))$  的基底。

**证明** 假定  $G$  的既约表现的代表系是  $\rho_1, \dots, \rho_q$ , 兹示明特征标  $\chi_{\rho_1}, \dots, \chi_{\rho_q}$  成为  $C(A(G))$  的基底即可。

由前定理,  $A(G) \cong \mathfrak{M}(d_1, \mathbb{C}) \oplus \dots \oplus \mathfrak{M}(d_q, \mathbb{C})$ .  $x \in A(G)$  到右边  $\mathfrak{M}(d_1, \mathbb{C}) \oplus \dots \oplus \mathfrak{M}(d_q, \mathbb{C})$  的同构映射, 象前定理的证明中

那样,用  $Q$  表示。由 § 26 定理 3 的系 1,  $\mathfrak{M}(d_v, C)$  的中心是  $\alpha E_{d_v}$ ,  $\alpha \in C$  形状的矩陣。再由前定理的証明得知  $Q^{-1}(E_{d_v})$  为

$$\sum_{i=1}^{d_v} e_{ii}^{(v)} = \frac{d_v}{n} \chi_{\rho_v}.$$

因此  $Q^{-1}(\mathfrak{M}(d_v, C))$  的中心能够用  $\chi_{\rho_v}$  生成。于是成为它們的直和的  $O(A(G))$  能够用  $\chi_{\rho_1}, \dots, \chi_{\rho_q}$  生成。因为  $\chi_{\rho_1}, \dots, \chi_{\rho_q}$  显然是无关,所以它們构成  $O(A(G))$  的基底。

例 3 假定  $f$  是  $O(A(G))$  中任意元,那末

$$f = \sum_{\nu=1}^q (f, \chi_{\rho_\nu}) \chi_{\rho_\nu}.$$

[解] 由  $(\chi_{\rho_\nu}, \chi_{\rho_\mu}) = \delta_{\nu\mu}$  显然①。

$A(G)$  中元  $f$  在  $G$  的共轭类上取一定值的,即对于任意  $x, y \in G$  满足  $f(x) = f(yxy^{-1})$  或  $f(yx) = f(xy)$  的函数,叫做  $G$  的类函数。例如特征标是类函数。假定把  $G$  类分为共轭类  $C_1, \dots, C_r$ , 含于  $C_\lambda$  ( $\lambda = 1, \dots, r$ ) 中元的个数是  $n_\lambda$  (于是  $\sum_{\lambda=1}^r n_\lambda = n(G)$  的阶)。如果把  $f \in A(G)$  象 § 29 命题 5 后面那样写成  $f = \sum_{x \in G} f(x)x$ , 那末对于类函数  $f$  自各类  $C_\lambda$  选代表元  $x_\lambda$ , 又命  $\sum_{x \in C_\lambda} x = X_\lambda$  就有  $f = \sum_{\lambda=1}^r f(x_\lambda) X_\lambda$ . 类函数的全部集合显然成为  $C$  上向量空间  $A(G)$  的子空间  $O'(A(G))$ , 因为  $X_\lambda$  是它的基底,所以它的維数等于  $r$ .

因为  $A(G)$  的中心  $O(A(G))$  中元显然是类函数,所以  $O(A(G)) \subset O'(A(G))$ . 另一方面,对于任意  $X_\lambda$  与任意  $a \in G$ ,  $aX_\lambda = \sum_{x \in C_\lambda} ax = \sum_{x \in C_\lambda} xa = X_\lambda a$ . 因为  $G$  中元看成为  $A(G)$  中元时是  $A(G)$  的基底,所以  $X_\lambda \in O(A(G))$ . 因此  $O'(A(G)) \subset O(A(G))$ . 于是  $O(A(G)) = O'(A(G))$ . 但  $\dim O(A(G))$  由前定理等于  $q$ ,

① 因为  $\chi_{\rho_1}, \chi_{\rho_2}, \dots, \chi_{\rho_q}$  是  $O(A(G))$  的一个基底,而  $f \in O(A(G))$ , 所以  $f = \sum_{\nu=1}^q a_\nu \chi_{\rho_\nu}$ . 两边对  $\chi_{\rho_\mu}$  求内积, 因为  $(\chi_{\rho_\nu}, \chi_{\rho_\mu}) = \delta_{\nu\mu}$ , 所以  $(f, \chi_{\rho_\mu}) = a_\mu$ . 因此  $f = \sum_{\nu=1}^q (f, \chi_{\rho_\nu}) \chi_{\rho_\nu}$ . ——譯者注

所以  $q=r$ , 于是就证明了下面的定理。

**定理 21** 有限群  $G$  的不等价既约表现的个数, 等于  $G$  的共轭类的个数。

**例 4**  $\mathfrak{S}_3$  的不等价既约表现的个数是 3 (例 1), 它等于  $\mathfrak{S}_3$  的共轭类的个数 (187 页例 2)。

由本节定理 19, 20, 则  $A(G)$ ,  $G(A(G))$  的构造是明显的。又由前节及本节有限群的表现能够用特征标较好的来规定。特别由最后的定理 21, 假如  $G$  有  $q$  个类  $C_1, \dots, C_q$ , 及  $q$  个单纯特征标  $\chi_{\rho_1}, \dots, \chi_{\rho_q}$ , 如果  $\chi_{\rho_\nu}$  在  $C_\lambda$  上所取的值是  $\alpha_{\nu\lambda}$ , 那就得到  $(q, q)$  型正方矩阵。但因为

类 \ 指标	$C_1$	$\dots$	$C_\lambda$	$\dots$	$C_q$
$\chi_{\rho_1}$	$\alpha_{11}$	$\dots$	$\alpha_{1\lambda}$	$\dots$	$\alpha_{1q}$
$\vdots$	$\vdots$		$\vdots$		$\vdots$
$\chi_{\rho_\nu}$	$\alpha_{\nu 1}$	$\dots$	$\alpha_{\nu\lambda}$	$\dots$	$\alpha_{\nu q}$
$\vdots$	$\vdots$		$\vdots$		$\vdots$
$\chi_{\rho_q}$	$\alpha_{q1}$	$\dots$	$\alpha_{q\lambda}$	$\dots$	$\alpha_{qq}$

$$\sum_{\lambda=1}^q n_\lambda \alpha_{\nu\lambda} \overline{\alpha_{\mu\lambda}} = n \delta_{\nu\mu} \quad \text{①}, \quad (33.2)$$

① 假设  $\rho_\nu, \rho_\mu$  是不等价的西的既约表现, 其表现矩阵分别为  $(a_{ij}^\nu(x)), (a_{ik}^\mu(x))$ , 因为  $a_{ki}^\mu(x^{-1}) = \overline{a_{ik}^\mu(x)}$ , 所以由 (31.2), (31.3) 即得

$$\sum_{x \in G} a_{ij}^\nu(x) \cdot \overline{a_{ik}^\mu(x)} = 0, \quad \text{当 } \nu \neq \mu, \quad (1)$$

$$\sum_{x \in G} a_{ij}^\nu(x) \cdot \overline{a_{ik}^\nu(x)} = \frac{n}{m} \delta_{jk} \delta_{il}, \quad \text{当 } \nu = \mu. \quad (2)$$

合并上两式即得等式  $\sum_{x \in G} a_{ij}^\nu(x) \cdot \overline{a_{ik}^\mu(x)} = \frac{n}{m} \delta_{jk} \delta_{il} \delta_{\nu\mu}$ .

假定  $\nu = \mu$ , 由 (2), 命  $j=i$  并对  $i$  求和得

$$\sum_{x \in G} \left( \sum_{i=1}^m a_{ii}^\nu(x) \cdot \overline{a_{ii}^\nu(x)} \right) = \frac{n}{m} \sum_{i=1}^m \delta_{ii} \delta_{ii} = \frac{n}{m} \delta_{kk} \delta_{ll}.$$

再令  $k=l$ , 并对  $k$  求和即得

$$\sum_{x \in G} \left( \sum_{i=1}^m \sum_{k=1}^m a_{ii}^\nu(x) \overline{a_{kk}^\nu(x)} \right) = \frac{n}{m} \cdot m = n.$$

即

$$\sum_{x \in G} \chi_{\rho_\nu}(x) \cdot \overline{\chi_{\rho_\mu}(x)} = n.$$

因为  $\chi_{\rho_\nu}$  是类函数, 所以

$$\sum_{\lambda=1}^q n_\lambda \alpha_{\nu\lambda} \overline{\alpha_{\mu\lambda}} = n.$$

当  $\nu \neq \mu$  时, 由 (1) 式出发用同样方法即可推出

$$\sum_{\lambda=1}^q n_\lambda \alpha_{\nu\lambda} \overline{\alpha_{\mu\lambda}} = 0.$$

所以 (33.2) 式成立。——译者注

命  $\sqrt{\frac{n_\lambda}{n}} \alpha_{\nu\lambda} = \beta_{\nu\lambda}$ , 那末  $(\beta_{\nu\lambda})$  成为酉矩陣。于是

$$\sum_{\nu=1}^q \beta_{\nu\lambda} \bar{\beta}_{\nu\kappa} = \delta_{\lambda\kappa},$$

所以 
$$\sum_{\nu=1}^q \alpha_{\nu\lambda} \bar{\alpha}_{\nu\kappa} = \frac{n}{n_\lambda} \delta_{\lambda\kappa}.$$

对于  $x, y \in G$ ,  $n_x = (x \text{ 所属的共轭类中元的个数})$ , 假如当  $x \sim y$  时, 命  $\delta_{xy} = 1$ , 当  $x \not\sim y$ , 命  $\delta_{xy} = 0$ , 那末

$$\sum_{\nu=1}^q \chi_{\rho_\nu}(x) \chi_{\rho_\nu}(y^{-1}) = \sum_{\nu=1}^q \chi_{\rho_\nu}(x^{-1}) \chi_{\rho_\nu}(y) = \frac{n}{n_x} \delta_{xy}. \quad (33.3)$$

在第二式特別命  $x = e$  得

$$\sum_{\nu=1}^q d_\nu \chi_{\rho_\nu}(y) = \begin{cases} n, & y = e, \\ 0, & y \neq e. \end{cases}$$

(33.3) 叫做特征标的第二直交关系, 与它相对, 也有把 § 32 定理 14 叫做第一直交关系的。在有限群的单纯特征标之間有如此的关系成立。

例 5 关于  $\mathfrak{S}_3$  的  $\alpha_{\nu\lambda}$  的表如下。特征标的第二直交关系由它容易推得。

			$C_1$	$C_2$	$C_3$
			(1)	(1 2), (1 3), (2 3)	(1 2 3), (1 3 2)
			$n_1=1$	$n_2=3$	$n_3=2$
恒等表现 $\rho_1$	$d_1=1$	$\chi_{\rho_1}$	1	1	1
交代表现 $\rho_2$	$d_2=1$	$\chi_{\rho_2}$	1	-1	1
2 級既約表现 $\rho_3$	$d_3=2$	$\chi_{\rho_3}$	2	0	-1

例 6 求  $\mathfrak{S}_4$  的所有单纯特征标。

[解] 象在 § 30 例 3 的表中所示, 因为  $\mathfrak{S}_4$  能够分为五个共轭类, 所以有五个既約表现。首先容易求得恒等表现  $\rho_1$  及交代表现  $\rho_2$  的特征标。一般, 某表现  $\sigma$  的特征标  $\chi_\sigma$  用 188 頁例 3 表中的記号, 在类  $C_1, C_2, C_3, C_4, C_5$  中所取的值分別是  $\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5$  时, 假如写成  $\chi_\sigma = (\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5)$ , 显然

$$\chi_{\rho_1} = (1, 1, 1, 1, 1), \chi_{\rho_2} = (1, -1, 1, 1, -1).$$

其次, 假如把 § 27 例 2 中开始所述的表现  $\rho$  (即对于  $\begin{pmatrix} 1 & 2 & \cdots & n \\ \nu_1 & \nu_2 & \cdots & \nu_n \end{pmatrix} \in G$  使矩阵  $x(\nu_1, \nu_2, \cdots, \nu_n)$  对应的  $n$  级忠实表现) 取为  $n=4$ , 那末①

$$\chi_\rho = (4, 2, 0, 1, 0).$$

与 § 27 例 2 同样考察能够分解  $\rho = \rho_1 \oplus \rho_3$ , 因为  $\chi_\rho = \chi_{\rho_1} + \chi_{\rho_3}$ , 所以

$$\chi_{\rho_3} = (3, 1, -1, 0, -1).$$

但因  $(\chi_{\rho_3}, \chi_{\rho_3}) = \frac{1}{4!}(1 \times 3^2 + 6 \times 1^2 + 3(-1)^2 + 8 \times 0^2 + 6(-1)^2) = 1$ , 所以  $\rho_3$  是既约。因为  $\rho_2$  是 1 级表现, 所以由 § 32 定理 16 系 2,  $\rho_4 = \rho_3 \otimes \rho_2$  又成为既约,

$$\chi_{\rho_4} = \chi_{\rho_3} \chi_{\rho_2} = (3, -1, -1, 0, 1).$$

于是  $\rho_5$  与  $\rho_1, \rho_2, \rho_3$  中任一都不等价。因为五个单纯特征标中四个已求出, 最后一个能够由第二直交关系求出。

表现 级数 $d_\rho$ 特征标 代表元 元的个数 $n_\lambda$ 类			$C_1$	$C_2$	$C_3$	$C_4$	$C_5$
			(1)	(12)	(12)(34)	(123)	(1234)
			1	6	3	8	6
$\rho_1$	1	$\chi_{\rho_1}$	1	1	1	1	1
$\rho_2$	1	$\chi_{\rho_2}$	1	-1	1	1	-1
$\rho_3$	3	$\chi_{\rho_3}$	3	1	-1	0	-1
$\rho_4$	3	$\chi_{\rho_4}$	3	-1	-1	0	1
$\rho_5$	2	$\chi_{\rho_5}$	2	0	2	-1	0

① 因为  $S_4$  的五个代表类为  $(1) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$ ,  $(12) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}$ ,  $(12)(34) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$ ,  $(123) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$ ,  $(1234) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$ . 所以  $(1) \rightarrow \begin{pmatrix} 1 & & & \\ & 1 & & \\ & & 1 & \\ & & & 1 \end{pmatrix}$ ,  $(12) \rightarrow \begin{pmatrix} 0 & 1 & & \\ 1 & 0 & & \\ & & 1 & \\ & & & 1 \end{pmatrix}$ ,  $(12)(34) \rightarrow \begin{pmatrix} 0 & 1 & & \\ 1 & 0 & & \\ & & 0 & 1 \\ & & 1 & 0 \end{pmatrix}$ ,  $(1234) \rightarrow \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}$ . 因此  $\chi_\rho = (4, 2, 0, 1, 0)$ . —译者注

## § 34 群的直积的表现

有限群  $G$  能够表为  $G_1, \dots, G_r$  的直积  $G_1 \otimes \dots \otimes G_r$  的形状时,  $G_i$  叫做  $G$  的直积因子。这时求  $G$  的表现的問題, 由下面定理 22 归結于关于各个直积因子  $G_i$  的問題。为了在定理証明的过程中不致中断, 首先把下面的命题 11 作为准备。

**命题 11** 假定  $G$  是有限群  $G_1, G_2$  的直积,  $G, G_i$  的共轭类的个数分别是  $q, q_i (i=1, 2)$ , 那末  $q = q_1 q_2$ 。

**証明**  $G$  中元  $x$  能够写成  $(x_1, x_2) (x_i \in G_i)$  的形状。假如  $y = (y_1, y_2)$ , 因为  $yxy^{-1} = (y_1 x_1 y_1^{-1}, y_2 x_2 y_2^{-1})$ , 所以, 如果  $\sim$  意味着属于同一共轭类, 那末  $(x_1, x_2) \sim (x'_1, x'_2) \Leftrightarrow x_1 \sim x'_1, x_2 \sim x'_2$ . 由这立即得到  $q = q_1 q_2$ 。

**定理 22** 假定  $G_1, G_2$  是有限群,  $G$  是它們的直积  $G_1 \otimes G_2$ ,  $\rho_i$  是  $G_i$  的表现,  $V_i$  是  $\rho_i$  的表现空間 ( $i=1, 2$ ). 这时  $G$  中元能够写成  $(x_1, x_2) (x_i \in G_i)$  形状, 如果  $V = V_1 \otimes V_2$ ,  $\rho(x) = \rho_1(x_1) \otimes \rho_2(x_2) \in GL(V)$ , 那末  $x \rightarrow \rho(x)$  是  $G$  在  $V$  的表现。这时成立

$$(1) \chi_\rho(x) = \chi_{\rho_1}(x_1) \cdot \chi_{\rho_2}(x_2).$$

(2)  $\rho$  是既約的必要充分条件是  $\rho_1, \rho_2$  都是既約。

假如  $G_i$  的既約表现的代表系是  $\rho_i^{(1)}, \dots, \rho_i^{(q_i)}$ , 那末  $q_1 q_2$  个  $G$  的表现  $\rho_1^{(j_1)} \otimes \rho_2^{(j_2)}$  ( $j_i=1, \dots, q_i$ ) 是  $G$  的既約表现的代表系。

**証明**  $x \rightarrow \rho(x)$  是  $G$  的表现及 (1), 由張量积的性质 (129 頁例 8 及 195 頁) 是显明的。

为了証明 (2), 首先証明下面的事实。假定  $\rho'_i$  是  $G_i$  的另一表现,  $\rho'_1 \otimes \rho'_2 = \rho'$ . 为了簡單, 命  $\chi_\rho = \chi, \chi_{\rho_i} = \chi_i, \chi_{\rho'} = \chi', \chi_{\rho'_i} = \chi'_i$ , 那末  $\chi, \chi'$  在  $A(G)$  的内积  $(\chi, \chi')$  成为  $\chi_i, \chi'_i$  在  $A(G_i)$  的内积  $(\chi_i, \chi'_i)$  的积, 即

$$(\chi, \chi') = (\chi_1, \chi'_1) (\chi_2, \chi'_2) \quad (34.1)$$

成立。实际上,假如  $G_i$  的阶是  $n_i$ , 因为  $G$  的阶是  $n = n_1 n_2$ , 所以

$$\begin{aligned} (\chi, \chi') &= \frac{1}{n} \sum_{x \in G} \chi(x) \overline{\chi'(x)} \\ &= \frac{1}{n_1 n_2} \sum_{\substack{x_1 \in G_1 \\ x_2 \in G_2}} \chi_1(x_1) \chi_2(x_2) \overline{\chi'_1(x_1) \chi'_2(x_2)} \\ &= \left( \frac{1}{n_1} \sum_{x_1 \in G_1} \chi_1(x_1) \overline{\chi'_1(x_1)} \right) \left( \frac{1}{n_2} \sum_{x_2 \in G_2} \chi_2(x_2) \overline{\chi'_2(x_2)} \right) \\ &= (\chi_1, \chi'_1) (\chi_2, \chi'_2). \end{aligned}$$

用它能够立即证明 (2)。由定理 16 系, “ $\rho$  既约  $\Leftrightarrow (\chi, \chi) = 1$ ”, “ $\rho_i$  既约  $\Leftrightarrow (\chi_i, \chi_i) = 1$ ”。因此,如果于 (34.1) 命  $\chi = \chi'$ ,  $\chi_i = \chi'_i$  就得到 “ $\rho_1, \rho_2$  既约  $\Rightarrow \rho$  既约”。又假如  $\rho_1$  或  $\rho_2$  是可约, 因为  $(\chi_1, \chi_1)$  或  $(\chi_2, \chi_2) > 1$ , 那末  $\rho$  也是可约。所以 (2) 成立。

于是  $\rho_1^{(j_1)} \otimes \rho_2^{(j_2)}$  都是既约的, 为了证明它们能够穷尽  $G$  的既约表现的代表类, 注意下面事实。假定  $\rho_i, \rho'_i$  是与上同样意义, 当  $\rho_i, \rho'_i$  是既约时,

$$\rho \sim \rho' \Leftrightarrow \rho_1 \sim \rho'_1, \rho_2 \sim \rho'_2$$

成立。这由 (34.1) 与特征标的直交性 (定理 14) 是显明的。所以  $q_1 q_2$  个  $G$  的既约表现  $\rho_1^{(j_1)} \otimes \rho_2^{(j_2)}$  属于相异的表类。但是由命题 11 及定理 21, 因为  $G$  的相异的既约表类的个数正好是  $q_1 q_2$ , 所以它们能够穷尽它的全部。

**系** 有限群  $G$  能够直积分解为  $G_1 \otimes \cdots \otimes G_r$  形状时,  $G$  的既约表现的代表系能够由各因子  $G_i$  的既约表现代表系所作的张量积表出。 (系毕)

例如引用 § 22 例 10 中所述的“可换群的基本定理”, 那末全部求有限可换群表现的问题由上定理立即得到解决。但这基本定理的证明没有叙述, 因此在这里对于有限群来补证。首先自下面的命题开始。

**命题 12** 假定  $G$  是阶为  $n$  的有限可换群。  $n = n_1 n_2, (n_1, n_2)$



$=1$ , 那末  $G$  中阶是  $n_1$  的約数的元全体的集合  $H_1$  成为  $G$  的子群, 并且  $G = H_1 \otimes H_2$ .

**証明** 先示  $H_1$  成为  $G$  的子群。假定  $x_1, y_1 \in H_1$  即  $x_1, y_1$  的阶都是  $n_1$  的約数, 因为  $(x_1 y_1^{-1})^{n_1} = x_1^{n_1} (y_1^{-1})^{n_1} = e$ , 所以  $x_1 y_1^{-1}$  的阶也是  $n_1$  的約数。于是  $x_1 y_1^{-1} \in H_1$ 。因为对于  $H_2$  也是一样, 所以  $H_i (i=1, 2)$  成为  $G$  的子群。因为  $G$  是可換群, 所以  $H_i$  是  $G$  的正規子群。这时当然  $H_1$  中元与  $H_2$  中元是可換。因此只要証明  $G$  中任意元  $x$  能够唯一地写成  $x = x_1 x_2, x_i \in H_i$  的形状即可。因为  $(n_1, n_2) = 1$ , 所以有滿足  $n_1 h_1 + n_2 h_2 = 1$  这样的  $h_1, h_2 \in \mathbb{Z}$  (157 頁, (ii))。于是  $x = x^{n_1 h_1} x^{n_2 h_2}$ , 但  $(x^{n_1 h_1})^{n_1} = x^{n_1 n_2 h_1} = x^{n_2 h_1} = e$ , 如果命  $x^{n_2 h_1} = x_1$ , 那末  $x_1 \in H_1$ 。同样  $x^{n_2 h_2} = x_2 \in H_2$ , 即任意  $x \in G$  能够表为  $x_1 x_2, x_i \in H_i$  的形状。再假如  $x_1 x_2 = y_1 y_2, x_i, y_i \in H_i$ , 如果命  $x_i y_i^{-1} = z_i$ , 那末  $z_i \in H_i, z_1 z_2 = e$ 。命  $z_1, z_2$  的阶分别是  $m_1, m_2$ , 那末  $m_i | n_i$ , 因而  $(m_1, m_2) = 1$ 。所以  $z_1 z_2$  的阶是  $m_1 m_2$  (158 頁引理 1)。今  $m_1 m_2 = 1$ , 所以  $m_1 = m_2 = 1$ 。即  $z_1 = z_2 = e$ , 这就証明了  $x = x_1 x_2$  表示方法的唯一性, 所以  $G = H_1 \otimes H_2$ 。

**系** 假如有限可換群  $G$  的阶  $n$  质因数分解成为  $n = p_1^{n_1} \cdots p_r^{n_r}$ , 那末  $G$  能够直积分解为  $H_1 \otimes \cdots \otimes H_r$  形状。但  $H_i$  是由  $G$  中阶为  $p_i^{n_i}$  的約数的元全体构成的  $G$  的子群。

**命題 13** 假定  $G$  是有限可換群, 如果  $G$  中异于  $e$  的任意元的阶都是质数  $p$ , 那末  $G$  是阶数  $p$  的循环群的直积,  $G$  的阶是  $p^r$  形状。

**証明** 在这命題的証明中, 开始把  $G$  的基本算法用加减法的形状写出。对于  $x \in G$ , 如果写  $x + x = 2x, 2x + x = 3x, \cdots$ , 那末  $px = 0$  ( $G$  的单位元)。于是对于  $\lambda \in \mathbb{Z}_p, x \in G$ , 則  $\lambda x \in G$  唯一的定义, 并且显然滿足 9 頁 B1~5。因为  $\mathbb{Z}_p$  是体 (§ 24 160 頁), 所以  $G$  是  $\mathbb{Z}_p$  上向量空間。但  $G$  是有限, 所以这向量空間的維数也有限,

如果它是  $r$ , 就具有  $r$  个基底  $a_1, \dots, a_r$  (22 页, 定理 5)。即  $G$  中任意元  $x$  能够唯一地写成  $\lambda_1 a_1 + \dots + \lambda_r a_r$ ,  $\lambda_i \in \mathbb{Z}_p$  的形状。因此, 如果变为普通乘法的记法, 那末  $x$  就能够唯一地表为  $a_1^{\lambda_1} \dots a_r^{\lambda_r}$  形状。 $H_i = \{e, a_i, a_i^2, \dots, a_i^{p-1}\}$  显然成为  $G$  的  $p$  阶循环子群, 而  $G = H_1 \otimes \dots \otimes H_r$ . 因为  $H_i$  的阶是  $p$ , 所以  $G$  的阶是  $p^r$ .

**命题 14** 假如有限可换群  $G$  中所有元的阶是质数幂  $p^\nu$  的约数, 那末  $G$  是把  $p$  的连乘作为阶数的循环群的直积 (因此  $G$  的阶也是  $p$  的连乘)。

**证明** 假定  $\nu = 1$ , 那末这命题就是前命题, 因此用关于  $\nu$  的归纳法, 对于  $\nu - 1$  假定命题已证明, 来证明  $\nu (\geq 2)$  的情况。

假定把  $G$  中各元  $p$  乘的集合  $\{x^p; x \in G\}$  用  $G^p$  表示, 那末  $G^p$  成为  $G$  的子群。实际上,  $x, y \in G$  时,  $x^p (y^p)^{-1} = (xy^{-1})^p \in G^p$ . 并且  $G^p$  中各元的阶显然是  $p^{\nu-1}$  的约数。所以由归纳法的假定,  $G^p$  是把  $p$  的连乘作为阶的循环群的直积。今假定  $G^p = H_1 \otimes \dots \otimes H_k$ ,  $H_i = \{e, a_i^p, a_i^{2p}, \dots, a_i^{p^{r_i-1}p}\}$  ( $r_i \geq 1$ ). 于是  $p^{r_i}$  是  $a_i^p$  的阶。因而  $a_i$  的阶是  $p^{r_i+1}$ . 命  $A_i = \{e, a_i, a_i^2, \dots, a_i^{p^{r_i+1}-1}\}$ ,  $A = A_1 \dots A_k$ , 显然  $A_i^p = H_i$ ,  $A^p = G^p$ ,  $A$  是用  $a_1, \dots, a_k$  生成的  $G$  的子群。要证明  $A = A_1 \otimes \dots \otimes A_k$ , 在这里只要证明

$$a_1^{\nu_1} \dots a_k^{\nu_k} = a_1^{\nu'_1} \dots a_k^{\nu'_k} \Rightarrow \nu_i = \nu'_i \pmod{p^{r_i+1}}$$

即可。由假定  $a_1^{\nu_1} \dots a_k^{\nu_k} = a_1^{\nu'_1} \dots a_k^{\nu'_k} \in H_1 \otimes \dots \otimes H_k$ . 所以  $\nu_i \equiv \nu'_i \pmod{p^{r_i}}$ . 今  $r_i \geq 1$ , 所以有满足  $\nu_i - \nu'_i = p\rho_i$  的  $\rho_i \in \mathbb{Z}$ . 因此由上式就得到  $a_1^{p\rho_1} \dots a_k^{p\rho_k} = e$ , 但  $a_i^p \in H_i$ ,  $H_1 \otimes \dots \otimes H_k$  是直积, 因此  $\rho_i \equiv 0 \pmod{p^{r_i}}$ . 所以  $\nu_i - \nu'_i = p\rho_i \equiv 0 \pmod{p^{r_i+1}}$ .

于是命  $G/A = H$ , 因为  $G \supset A \supset A^p = G^p$ , 所以  $G$  中任意元如果  $p$  乘就在  $A$  中, 因此,  $H$  中任意元如果  $p$  乘即成为  $H$  的单位元  $E = A$ . 所以  $H = E$  或  $H$  成为满足命题 13 中假设的 (不是单位群) 群。当  $H = E$  时, 因为  $G = A = A_1 \otimes \dots \otimes A_k$ , 这样就达到了目

的。在后面情况, 假定  $H = K_1 \otimes \cdots \otimes K_l$ ,  $K_j = \{E, B_j, B_j^2, \dots, B_j^{p-1}\}$  ( $j=1, \dots, l$ ), 如果  $b_j \in B_j$ . 因为  $b_j^p \in G^p = A^p$ , 取适当的  $c_j \in A$ , 那末  $b_j^p = c_j^p$ . 因此命  $d_j = b_j c_j^{-1}$ , 就得到  $d_j \in B_j$ ,  $d_j^p = e$ .  $G$  中任意元  $x$  显然能够写成

$$x = a_1^{\lambda_1} \cdots a_k^{\lambda_k} d_1^{\mu_1} \cdots d_l^{\mu_l}$$

$$(\lambda_i = 0, 1, \dots, p^{r_i+1} - 1; \mu_j = 0, 1, \dots, p-1), \quad (34.2)$$

又因为  $\lambda_i, \mu_j$  在上面范围内变动正好是  $p$  的  $(\sum_{i=1}^k (r_i+1) + l)$  乘, 即正好能够得到  $(A:1) \cdot (H:1) = (G:1)$  个元, 所以  $G$  中元象 (34.2) 那样的表示方法是唯一的。于是命  $D_j = \{e, d_j, \dots, d_j^{p-1}\}$  就得到  $G = A_1 \otimes \cdots \otimes A_k \otimes D_1 \otimes \cdots \otimes D_l$ . (证毕)

由命题 12 的系及上面的命题 14 得出下面“关于有限可换群的基本定理”。

**定理 23** 有限可换群能够表为循环群的直积。

**例 1** (1) 命题 12 中  $H_i$  的阶是  $n_i$ .

(2) 命题 12 系中  $H_i$  的阶是  $p_i^{v_i}$ .

[解] 证明(2)这方即可。由命题 14,  $H_i$  的阶是  $p_i$  的连乘  $p_i^{v_i}$ . 因为  $G = H_1 \otimes \cdots \otimes H_k$ , 所以  $G$  的阶  $n = p_1^{v_1} \cdots p_k^{v_k} = p_1^{v'_1} \cdots p_k^{v'_k}$ . 由质因数分解的唯一性,  $v'_i = v_i (i=1, \dots, k)$ .

由定理 23, 任意有限可换群  $G$  能够用循环群  $G_1, \dots, G_r$  的直积  $G_1 \otimes \cdots \otimes G_r$  的形状写出。因此, 假如  $G_i$  的生成元是  $a_i$ , 它的阶是  $n_i$ , 那末  $G$  中任意元  $x$  能够唯一地表为

$$x = a_1^{v_1} a_2^{v_2} \cdots a_r^{v_r}.$$

$\{a_1, \dots, a_r\}$  叫做  $G$  的基底。上面定理叫做可换群的基底定理。

**例 2** 四元群 (Klein 的四元群 Vierergruppe)。

由  $1, a = (1\ 2)(3\ 4), b = (1\ 3)(2\ 4), c = (1\ 4)(2\ 3)$  四个元构成的  $\mathfrak{S}_4$  的子群  $G$ , 叫做四元群。这群  $G$  的群表如左。它显然是可换群。假定  $G_1 = \{1,$

	1	a	b	c
1	1	a	b	c
a	a	1	c	b
b	b	c	1	a
c	c	b	a	1

$a\}$ ,  $G_2 = \{1, b\}$ ,  $G_3 = \{1, c\}$ , 那末它們都是  $G$  的阶 2 的循环子群, 而  $G = G_1 \otimes G_2 = G_2 \otimes G_3 = G_3 \otimes G_1$ .  $G$  的基底能够取  $\{a, b\}$ ,  $\{b, c\}$ ,  $\{c, a\}$  中任一个。(象这样, 基底的取法一般不是唯一的。)

由 170 頁的例与上定理 22 的系, 及定理 23 立即得到下面关于有限可換群的既約表現的結論。

**定理 24** 假定  $G$  是有限可換群,  $G = G_1 \otimes \cdots \otimes G_r$  是  $G$  的循环群  $G_i (i=1, \cdots, r)$  的直积分解。如果  $G_i$  的阶是  $n_i$ , 它的生成元是  $a_i$ , 命  $\zeta_i = \exp(2\pi\sqrt{-1}/n_i)$ , 那末  $G$  的既約表現都是 1 級, 由

$$G \ni x = a_1^{m_1} \cdots a_r^{m_r} \rightarrow \chi_{m_1, \dots, m_r}(x) = \zeta_1^{m_1} \cdots \zeta_r^{m_r}$$

給出。这里  $m_i$  在  $\text{mod } n_i$  的剩余类上变动 ( $i=1, \cdots, r$ )。

**注意** 假如  $m_i$  分別取  $0, 1, \cdots, n_i-1$  的值, 就得到  $G$  所有的既約表現。因此  $G$  的既約表現的个数是  $n_1 n_2 \cdots n_r = n$  ( $G$  的阶) (这由 § 30 例 1 及 § 33 定理 21 自明)。象 § 32 中注意那样, 这时  $G$  的既約表現与  $G$  的特征标一致。把  $G$  的特征标的集合用  $G^*$  表示, 如果  $\chi_{m_1, \dots, m_r}, \chi_{m'_1, \dots, m'_r} \in G^*$  的积用  $\chi_{m_1+m'_1, \dots, m_r+m'_r}$  定义, 那末  $G^*$  也成为可換群。 $G^*$  显然与  $G$  同构。 $G^*$  叫做  $G$  的特征标群,  $G \cong G^*$  这事实, 叫做关于可換群的特征标群的对偶定理。

## § 35 誘導表現

假定  $G$  是任意群,  $H$  是它的子群, 給出  $H$  的一个表現  $\sigma$ , 这时能够象下面那样作出  $G$  的表現  $\rho$ 。

假定  $U$  是  $\sigma$  的表現空間, 在把  $G$  作为定义域, 取  $U$  中值的函数  $f, g, \cdots$  的集合  $W$  中, 如果由

$$\begin{aligned} (f+g)(a) &= f(a) + g(a) & (a \in G), \\ (\lambda f)(a) &= \lambda f(a) & (a \in G, \lambda \in \mathbb{C}) \end{aligned}$$

引入綫性算法, 那末  $W$  成为 ( $\mathbb{C}$  上) 向量空間。假如对于任意  $a \in G$ ,  $b \in H$ , 滿足

$$f(ba) = \sigma(b)f(a) \quad (35.1)$$

的  $W$  中元  $f$  的集合是  $V$ , 那末  $V$  显然成为  $W$  的子空間。今对

$x \in G$ , 写成  $f(ax) = f_x(a)$ , 显然  $f_x \in W$ , 假如  $f \in V$ , 因为  $f_x(ba) = f(bax) = \sigma(b)f(ax) = \sigma(b)f_x(a)$ , 所以  $f_x \in V$ . 假如由  $\rho(x)f = f_x$  来定义  $\rho(x)$ , 那就立刻得知  $\rho(x): V \rightarrow V$ ,  $\rho(x) \in GL(V)$ , 并且

$$\rho(xy^{-1}) = \rho(x)\rho(y)^{-1}.$$

因此  $\rho$  成为  $G$  把  $V$  作为表现空間的表现。这  $\rho$  叫做由  $\Pi$  的表现  $\sigma$  诱导的  $G$  的诱导表现。

今假定  $G$  是  $n$  阶有限群,  $H$  是它的  $h$  阶子群,  $n = hk$ , 于是  $(G:H) = k$ . 把  $G$  类分为关于  $\text{mod } H$  的右剩余类, 假定

$$G = Ha_1 + \cdots + Ha_k,$$

又假定  $\dim U (= \sigma \text{ 的級数}) = m$ ,  $u_1, \dots, u_m$  是  $U$  的一个基底, 这时命

$$\begin{cases} f_{ij}(a_l) = \delta_{il}u_j, \\ f_{ij}(ba_l) = \sigma(b)f_{ij}(a_l), \text{ 对于 } b \in H, \end{cases}$$

那末  $f_{ij}(x)$ ,  $x \in G$ , 已定义, 容易得知  $f_{ij} \in V$ . 并且这等  $f_{ij}$ ,  $i = 1, \dots, h, j = 1, \dots, m$  成为  $V$  的基底。实际上, 假如  $f$  是  $V$  中任意元, 如果

$$f(a_l) = \sum_{j=1}^m \lambda_{lj}u_j,$$

显然因为  $f = \sum_{ij} \lambda_{ij}f_{ij}$  ①, 所以  $V$  能够用  $f_{ij}$  生成, 又因为  $\sum \lambda_{ij}f_{ij} = 0 \Rightarrow \lambda_{ij} = 0$ , 所以  $f_{ij}$  是无关。于是  $\rho$  的級数  $= \dim V = mk$ .

再假定  $\{u_1, \dots, u_m\}$  是  $U$  的基底时, 表示  $\sigma(b)$  的矩阵是  $\Sigma(b) = (s_{\mu\nu}(b))$ , 取上面  $V$  的基底  $f_{11}, \dots, f_{km}$  来考虑表示  $\rho(x)$  的矩阵  $P(x)$  应该成为如何形状?

对于  $x \in G$ , 因为  $a_l x$  在关于  $\text{mod } H$  的某右剩余系中, 假定它是  $Ha_{l'}$ .  $l' = l'(x, l)$  是  $x$  与  $l$  的函数,  $l'(x, 1), \dots, l'(x, k)$  是

① 因为  $f, \sum_{ij} \lambda_{ij}f_{ij}$  是  $G$  对于  $H$  的分类的类函数, 所以比較它們在  $a_l (l=1, 2, \dots, k)$  的值即知它們相等。——譯者注



上面的  $s_{\mu\nu}$  可以看成  $A(H)$  中元, 对于  $b \in H$  被定义取  $C$  中值的函数, 更一般对于  $g \in A(H)$ ,  $x \in G$ , 由

$$g^0(x) = \begin{cases} g(x), & x \in H, \\ 0, & x \notin H \end{cases}$$

定义  $g^0 \in A(G)$ , 命

$$P_{\kappa\lambda}(x) = (s_{\mu\nu}^0(a_\kappa x a_\lambda^{-1})) \quad (\kappa, \lambda = 1, \dots, k),$$

那末

$$P(x) = \begin{pmatrix} P_{11}(x) & \cdots & P_{1k}(x) \\ \vdots & & \vdots \\ P_{k1}(x) & \cdots & P_{kk}(x) \end{pmatrix}.$$

实际上, 假如  $\lambda \neq \nu$ , 那末  $P_{\mu\lambda}(x) = (s_{\mu\nu}^0(a_\nu x a_\lambda^{-1})) = O_{m_\mu, m_\nu}$ ,  $P_{\mu\nu}(x) = (s_{\mu\nu}(a_\nu x a_\nu^{-1})) = \Sigma(b_i)$ , 所以上述成立。

特別<sup>①</sup>,

$$(\chi_\rho x) = SP(x) = \sum_{\kappa=1}^k SP_{\kappa\kappa}(x) = \frac{1}{h} \sum_{\sigma \in G} \chi_\sigma^0(axa^{-1}). \quad (35.2)$$

例1 假如  $H = \{e\}$ , 那末  $\rho$  是右正则表现, 假如  $G = H$ , 那末  $\rho \sim 0$ .

例2  $G = \mathfrak{S}_3$  的子群  $H = \{1, (12)\}$  的既约表现有恒等表现, 交代表现两个。求分别由它们诱导的  $G$  的表现  $\rho^{(1)}$ ,  $\rho^{(2)}$ , 假定  $G = H \cdot 1 + H \cdot (13) + H \cdot (23)$ , 求  $G$  由  $H$  的交代表现诱导的矩阵表现即得下面的结果。

① 因为  $\chi_\rho(x) = \sum_{\kappa=1}^k SP_{\kappa\kappa}(x)$ , 这里  $P_{\kappa\kappa}(x) = 0$ , 当  $\nu(\kappa) \neq \kappa$ ,  $P_{\kappa\kappa}(x) = (s_{\nu\mu}(b_{\nu(\kappa)}))$ , 当  $\nu(\kappa) = \kappa$ . 但这时  $a_\kappa x = b_\kappa a_\nu$  所以  $a_\kappa x = b_\kappa a_\kappa$  因此  $b_\kappa = a_\kappa x a_\kappa^{-1}$ . 于是只有存在  $a_\kappa$  使  $b_\kappa = a_\kappa x a_\kappa^{-1} \in H$  时  $\chi_\rho(x) \neq 0$  并且

$$\chi_\nu(x) = SP_{\kappa\kappa}(x) = \chi_\sigma(b_\kappa) = \chi_\sigma(a_\kappa x a_\kappa^{-1})$$

又因为, 假如  $a_\kappa x a_\kappa^{-1} \in H$ , 那末对于任意  $H$  中元  $y$ ,  $(y a_\kappa) x (y a_\kappa^{-1}) \in H$ . 显然  $a_\kappa x a_\kappa^{-1}$  与  $(y a_\kappa) x (y a_\kappa^{-1})^{-1}$  共轭并且都属于  $H$ . 因为  $y$  有  $h$  个, 所以

$$\chi_\rho(x) = \frac{1}{h} \sum_{y \in H} \chi_\sigma((y a_\kappa) x (y a_\kappa^{-1})).$$

假如令  $g^0(x) = \begin{cases} g(x), & \text{当 } x \in H \\ 0, & \text{当 } x \notin H, \end{cases}$  那末上式可记成  $\chi_\rho(x) = \frac{1}{h} \sum_{\sigma \in G} \chi_\sigma^0(axa^{-1})$ . 实际

上, 如果  $\nu(\kappa) = \kappa$ , 那末上式中的  $a$  必为  $y a_\kappa$ ,  $y \in H$  的形状, 否则  $\chi_\sigma^0(axa^{-1}) = 0$ . ——  
譯者注

$$\begin{aligned}
P^{(2)}(1) &= \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, & P^{(2)}((1\ 2)) &= \begin{pmatrix} -1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & -1 & 0 \end{pmatrix}, \\
P^{(2)}((1\ 3)) &= \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix}, & P^{(2)}((2\ 3)) &= \begin{pmatrix} 0 & 0 & 1 \\ 0 & -1 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \\
P^{(2)}((1\ 2\ 3)) &= \begin{pmatrix} 0 & 0 & -1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, & P^{(2)}((1\ 3\ 2)) &= \begin{pmatrix} 0 & -1 & 0 \\ 0 & 0 & 1 \\ -1 & 0 & 0 \end{pmatrix}.
\end{aligned}$$

$P^{(1)}$  显然能够将  $P^{(2)}$  中  $-1$  都用  $1$  替换得出。因此

$$\chi_{\rho^{(1)}} = (3, 1, 0), \quad \chi_{\rho^{(2)}} = (3, -1, 0).$$

把它与 § 33 例 5 的表比较, 显然有下面关系

$$\rho^{(1)} = \rho_1 \oplus \rho_3, \quad \rho^{(2)} = \rho_2 \oplus \rho_3.$$

这里,  $\rho_1, \rho_2, \rho_3$  分别是  $G$  的恒等表现, 交代表现, 2 级既约表现。

对于上面的  $g \in A(H)$  使  $g^0 \in A(G)$  对应的映射是自  $A(H)$  到  $A(G)$  中的同构映射, 但对于  $f \in A(G)$  使它到  $H$  的缩小  $f|_H = \hat{f}$  对应的映射是自  $A(G)$  到  $A(H)$  上的同态映射。

**例 3** 假定  $\rho$  是  $G$  的任意表现, 那末  $\rho$  到  $H$  的缩小  $\rho|_H = \hat{\rho}$  给出  $H$  的表现 ( $\hat{\rho}$  的表现空间与  $\rho$  的相同, 但  $\rho$  是既约,  $\hat{\rho}$  不一定是既约)。如果  $\rho$  的矩阵表现是  $G \ni x \rightarrow P(x) = (p_{ij}(x))$ , 那末  $\hat{\rho}$  的一个矩阵表现能够用  $H \ni y \rightarrow \hat{P}(y) = (\hat{p}_{ij}(y))$  给出。

对于  $g \in A(H)$ , 命  $g^0 = f$ , 显然  $\hat{f} = \hat{g}^0|_H = g$ , 但对于  $f \in A(G)$ , 如果命  $\hat{f} = g$ , 一般  $g^0 = \hat{f}^0$  与  $f$  不相同。这是因为  $f$  与  $\hat{f}^0$  对于  $H$  中元取相同的值, 但对于  $x \notin H$  的  $x$ ,  $\hat{f}^0(x) = 0$ , 而  $f(x)$  一般不为  $0$  ( $x \notin H \Rightarrow f(x) = 0$  时, 并且限于这时,  $f = \hat{f}^0$ )。于是下面的命题成立。

**命题 15**  $g_1 \in A(H)$  时,  $fg_1^0 = \hat{f}^0 g_1^0$ 。

**证明** 假如  $x \notin H$ , 那末  $f(x)g_1^0(x) = \hat{f}^0 g_1^0(x) = 0$ 。假如  $y \in H$ , 那末  $f(y)g_1^0(y) = \hat{f}^0(y)g_1^0(y) = f(y)g_1(y)$ 。 (証毕)

假定  $G, H$  的类函数 (§ 33) 的全体分别用  $C(G), C(H)$  表



示, 那末  $C(G)$ ,  $C(H)$  分別是  $A(G)$ ,  $A(H)$  的可換子環。如果  $g \in C(H)$ , 不一定  $g^0 \in C(G)$ , 但

$$g^*(a) = \frac{1}{h} \sum_{x \in G} g^0(xax^{-1})$$

是  $C(G)$  中元。  $g \rightarrow g^*$  成為自  $C(H)$  到  $C(G)$  中的綫性映射。

**例 4** 用這記法, 上式 (35.1) 能够寫成下面形狀。假如  $G$  由  $H$  的表現  $\sigma$  誘導的表現是  $\rho$ , 那末

$$\chi_\rho = \chi_{\sigma^*}.$$

在  $A(G)$  中, 對於  $f_1, f_2 \in A(G)$ , 能够由

$$(f_1, f_2) = \frac{1}{n} \sum_{x \in G} f_1(x) \overline{f_2(x)}$$

定義內積 (§ 31)。與這同樣意義, 在  $A(H)$  定義的內積用

$$\langle g_1, g_2 \rangle = \frac{1}{h} \sum_{y \in H} g_1(y) \overline{g_2(y)}, \quad g_1, g_2 \in A(H)$$

表示。這時下面的定理成立。

**定理 25** 假定  $f, g$  分別是  $C(G)$ ,  $C(H)$  中任意兩元, 那末

$$(f, g^*) = \langle \hat{f}, g \rangle$$

成立。

它叫做 Frobenius 的相互律。

證明中需用下面的引理。

**引理** 對於  $G$  中任意元  $y$ , 使  $xax^{-1} = y$  這樣的  $G$  中元  $a, x$  的組  $(a, x)$  正好只有  $n (= G$  的階) 個。

**證明**  $x$  自  $G$  中任意取, 如果  $a = x^{-1}yx$ , 那末  $xax^{-1} = y$ 。又要  $xax^{-1} = y$  成立, 必須  $a = x^{-1}yx$ 。

**定理 25 的證明** 由  $g^*$  的定義,  $f$  是類函數及由命題 15 得

$$\begin{aligned} f(a) \overline{g^*(a)} &= \frac{1}{h} \sum_{x \in G} f(a) \overline{g^0(xax^{-1})} = \frac{1}{h} \sum_{x \in G} f(xax^{-1}) \overline{g^0(xax^{-1})} \\ &= \frac{1}{h} \sum_{x \in G} \hat{f}^0(xax^{-1}) \overline{g^0(xax^{-1})}, \end{aligned}$$

所以

$$(f, g^*) = \frac{1}{nh} \sum_{x \in G} \sum_{x \in G} \hat{f}^0(xax^{-1}) \overline{\hat{g}^0(xax^{-1})}. \quad (35.3)$$

在这右边的各項中，如果  $xax^{-1} \notin H$ ，它就是 0，如果  $xax^{-1} = y \in H$ ，它就取与  $\hat{f}(y) \overline{\hat{g}(y)}$  相同的值。并且对于給出的  $y \in H$  满足  $xax^{-1} = y$  这样的組  $(a, x)$  的个数由引理正好只有  $n$  个。把(35.3)中右边关于这  $n$  个  $(a, x)$  組的項先平均就得到

$$(f, g^*) = \frac{1}{h} \sum_{y \in H} \hat{f}(y) \overline{\hat{g}(y)} = \langle \hat{f}, \hat{g} \rangle.$$

**系 1** 假定  $\rho$  是由  $H$  的表現  $\sigma$  誘導的  $G$  的表現，如果  $f$  是  $A(G)$  中任意元，那末

$$(f, \chi_\rho) = \langle \hat{f}, \chi_\sigma \rangle.$$

**系 2** 假定  $\rho_i$  是  $G$  的既約表現， $\sigma$  是  $H$  的既約表現，如果  $\rho$  是由  $\sigma$  誘導的  $G$  的表現，那末

$$(\rho : \rho_i) = (\hat{\rho}_i : \sigma).$$

即在把  $G$  的既約表現  $\rho_i$  縮小到子群  $H$  所得到的表現  $\hat{\rho}_i$  中， $H$  的既約表現  $\sigma$  的重复度等于在由  $\sigma$  誘導的  $G$  的表現  $\rho$  中  $\rho_i$  的重复度(也有叫这系做 Frobenius 的相互律的)。

**証明** 由系 1 与 § 32 的命題 10 即得。

**例 5** 假定  $G$  的共軛类是  $C_1, \dots, C_q$ ,  $H$  是  $G$  的子群，如果  $H$  中两元  $y_1, y_2$  在  $H$  共軛——即存在  $y_1 = yy_2y^{-1}$ ,  $y \in H$  这样的  $y$ ——当然  $y_1, y_2$  在  $G$  中也是共軛并且属于同一共軛类。反之， $H$  中两元在  $G$  中虽为共軛，但在  $H$  中不一定成为共軛。因此，假如  $H$  的共軛类是  $D_1, \dots, D_r$ ，那末  $C_i \cap H$  就成为几个  $D_j$  的和的集合。今命  $C_i \cap H = D_{j_1}^{(\varphi_i)} + \dots + D_{j_s}^{(\varphi_i)}$ ,  $\varphi_i$  是  $C_i$  的定义函数，即

$$\varphi_i(x) = \begin{cases} 1, & x \in C_i, \\ 0, & x \notin C_i \end{cases}$$

是  $A(G)$  中元，假如  $C_i$  中元的个数是  $n_i$ ，由  $H$  的表現  $\sigma$  誘導的  $G$  的表現是  $\rho$ ，那末对于  $x_i \in C_i$ ,

$$\chi_\rho(x_i) = \frac{n}{n_i} (\chi_\rho, \varphi_i) = \frac{n}{n_i} \langle \chi_\sigma, \hat{\varphi}_i \rangle.$$

假如  $D_j$  中元的个数是  $m_j$ ,  $D_f \ni y_j$ , 由这即得

$$\chi_\rho(x_i) = \frac{n}{n_f h} (m_{j_1^{(i)}} \chi_\rho(y_{j_1^{(i)}}) + \cdots + m_{j_h^{(i)}} \chi_\rho(y_{j_h^{(i)}})).$$

**例 6** 5 阶交代群。

5 阶交代群用  $\mathfrak{A}_5$  表示。(因为  $\mathfrak{A}_5$  与使正 20 面体重合于它自身的运动所形成的群 (143 頁) 同构, 所以也叫做正 20 面体群。)  $\mathfrak{A}_5$  由下面 60 个置换构成 (以下表示共轭类分类,  $C_i$ ,  $i=1, \dots, 5$  是类的記号)。

$C_1: 1$	元的个数 1
$C_2: (1\ 2)(3\ 4), \dots$	15
$C_3: (1\ 2\ 3), \dots$	20
$C_4: (1\ 2\ 3\ 4\ 5), \dots$	12
$C_5: (1\ 3\ 5\ 2\ 4), \dots$	12

(上面的  $C_4, C_5$  在 5 阶对称群  $\mathfrak{S}_5$  中是同类, 但在  $\mathfrak{A}_5$  中则属于异类。因为  $\mathfrak{S}_5 = \mathfrak{A}_5 + \mathfrak{A}_5(1\ 2)$ , 所以  $x, y \in \mathfrak{A}_5$  在  $\mathfrak{S}_5$  中虽属同类, 当  $y = (1\ 2)x(1\ 2)$  时, 在  $\mathfrak{A}_5$  中不一定属于同类)。

因为  $\mathfrak{A}_5$  能够类分为这五个共轭类, 所以有五个相异的既約表现类。假定它们的代表系是  $\rho_i$ ,  $i=1, \dots, 5$ 。特别, 把  $\rho_1$  作为恒等表现,

$$\chi_{\rho_1} = (1, 1, 1, 1, 1).$$

第 2 既約表现  $\rho_2$ , 能够与  $\mathfrak{S}_3, \mathfrak{S}_4$  的情况 (176 頁, 202 頁) 同样求得。即对  $\pi \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ \nu_1 & \nu_2 & \nu_3 & \nu_4 & \nu_5 \end{pmatrix} \in \mathfrak{A}_5$  使  $\pi(\nu_1, \nu_2, \nu_3, \nu_4, \nu_5)$  对应的表现假如是  $\rho$ , 那末

$$\chi_\rho = (5, 1, 2, 0, 0).$$

与 203 頁同样考察, 因为  $\rho$  含  $\rho_1$  是明显的, 所以如果  $\rho = \rho_1 \oplus \rho_2$ , 那末

$$\chi_{\rho_2} = (4, 0, 1, -1, -1).$$

因为  $(\chi_{\rho_1}, \chi_{\rho_2}) = 1$ , 所以  $\rho_2$  是第 2 既約表现。

为了求剩下的三个既約表现, 假定由  $a = (1\ 2\ 3\ 4\ 5) \in \mathfrak{A}_5$  生成的  $\mathfrak{A}_5$  的子群是  $H$ , 因为  $H = \{1, a, a^2, a^3, a^4\}$  是 5 阶循环群, 如果命  $\varepsilon = e^{\frac{2\pi i}{5}}$ , 那末由

$$\sigma_\mu(a) = \varepsilon^\mu, \quad \sigma_\mu(a^\nu) = \varepsilon^{\mu\nu} \quad (\mu, \nu = 0, 1, 2, 3, 4)$$

能够得到  $H$  的所有既約表现。假定由这等表现誘导的  $\mathfrak{A}_5$  的表现是  $\rho^{(\mu)}$ , 那末  $\rho^{(\mu)}$  是 12 級表现。下面求  $\rho^{(\mu)}$  的特征标。

因为  $H$  是可换群, 所以它的共轭类都是只由一个元构成。因此  $H$  类分为五个共轭类, 与  $C_i$  的关系列示如下:

$$\begin{array}{ccccccc}
\mathfrak{A}_5 = C_1 + C_2 + C_3 & & + C_4 & & + C_5 \\
\cup & \cup & & \subset & \supset & & \subset & \supset \\
H = \{1\} & & + \{\alpha\} & + \{\alpha^4\} & + \{\alpha^2\} & + \{\alpha^3\} \\
\chi_{\sigma_\mu} = 1 & & \varepsilon^\mu & \varepsilon^{4\mu} & \varepsilon^{2\mu} & \varepsilon^{3\mu}
\end{array}$$

于是由例 5 得

$$\begin{aligned}
\chi_{\rho^{(0)}} &= \left( \frac{60}{1 \times 5} \times 1, 0, 0, -\frac{60}{12 \times 5} (\varepsilon^\mu + \varepsilon^{4\mu}), -\frac{60}{12 \times 5} (\varepsilon^{2\mu} + \varepsilon^{3\mu}) \right) \\
&= (12, 0, 0, \varepsilon^\mu + \varepsilon^{-\mu}, \varepsilon^{2\mu} + \varepsilon^{-2\mu}).
\end{aligned}$$

命  $\mu = 0, 1, 2, 3, 4, 5$ , 因为  $\chi_{\rho^{(1)}} = \chi_{\rho^{(5)}}$ ,  $\chi_{\rho^{(2)}} = \chi_{\rho^{(3)}}$ , 所以得到下面三个特征标

$$\begin{aligned}
\chi_{\rho^{(0)}} &= (12, 0, 0, 2, 2), \\
\chi_{\rho^{(1)}} &= \left( 12, 0, 0, -\frac{1+\sqrt{5}}{2}, -\frac{1-\sqrt{5}}{2} \right), \\
\chi_{\rho^{(2)}} &= \left( 12, 0, 0, -\frac{1-\sqrt{5}}{2}, -\frac{1+\sqrt{5}}{2} \right).
\end{aligned}$$

它們不是单纯特征标。于是在这等表現中計算既得的既約表現  $\rho_1, \rho_2$  的重复度, 把  $\rho^{(0)}, \rho^{(1)}, \rho^{(2)}$  更分解

$$\begin{aligned}
(\rho^{(0)} : \rho_1) &= (\chi_{\rho^{(0)}}, \chi_{\rho_1}) = \frac{1}{60} (1 \times 12 \times 1 - 1 \times 2 \times 12 + 1 \times 2 \times 12) = 1, \\
(\rho^{(0)} : \rho_2) &= (\chi_{\rho^{(0)}}, \chi_{\rho_2}) = \frac{1}{60} (4 \times 12 \times 1 + (-1) \times 2 \times 12 + (-1) \\
&\quad \times 2 \times 12) = 0,
\end{aligned}$$

所以分解  $\rho^{(0)} = \rho_1 \oplus \rho'_1$ ,

$$\chi_{\rho'_1} = \chi_{\rho^{(0)}} - \chi_{\rho_1} = (11, -1, -1, 1, 1).$$

$\rho'_1$  已不含  $\rho_1, \rho_2$ . 因为  $(\chi_{\rho'_1}, \chi_{\rho_1}) = 3$ , 所以  $\rho'_1$  是剩下的三个既約表現  $\rho_3, \rho_4, \rho_5$  的直和 (假如  $\rho'_1 = m_1 \rho_3 \oplus m_2 \rho_4 \oplus m_3 \rho_5$ , 那末  $(\chi_{\rho'_1}, \chi_{\rho_1}) = m_1^2 + m_2^2 + m_3^2$ , 因为  $m_i$  是非負的整数, 所以不得不  $m_1 = m_2 = m_3 = 1$ ). 又因为  $(\rho^{(1)} : \rho_1) = 0$ ,  $(\rho^{(1)} : \rho_2) = 1$ , 所以分解  $\rho^{(1)} = \rho_2 \oplus \rho'_2$ ,  $\rho'_2$  不含  $\rho_1, \rho_2$ .

$$\chi_{\rho'_2} = \chi_{\rho^{(1)}} - \chi_{\rho_2} = \left( 8, 0, -1, \frac{1+\sqrt{5}}{2}, \frac{1-\sqrt{5}}{2} \right).$$

因为  $(\chi_{\rho'_2}, \chi_{\rho_1}) = 2$ , 所以  $\rho'_2$  是  $\rho_3, \rho_4, \rho_5$  中两个的直和。譬如  $\rho'_2 = \rho_4 \oplus \rho_5$ , 那末

$$\chi_{\rho_3} = \chi_{\rho'_2} - \chi_{\rho_4} = \left( 3, -1, 0, -\frac{1-\sqrt{5}}{2}, \frac{1+\sqrt{5}}{2} \right).$$

同样, 因为  $(\rho^{(2)}: \rho_1) = 0$ ,  $(\rho^{(2)}: \rho_2) = 1$ , 所以  $\rho^{(2)} = \rho_2 \oplus \rho_3^*$ ,

$$\chi_{\rho_3} = \left( 8, 0, -1, \frac{1-\sqrt{5}}{2}, \frac{1+\sqrt{5}}{2} \right).$$

因为  $(\chi_{\rho_3}, \chi_{\rho_1}) = 2$ , 所以

$$\chi_{\rho_1} - \chi_{\rho_3} = \left( 3, -1, 0, \frac{1+\sqrt{5}}{2}, \frac{1-\sqrt{5}}{2} \right),$$

它又是单纯特征标。因为它与  $\rho_3$  不同, 所以是第 4 个既约表现  $\rho_4$  的特征标。

最后一个特征标能够由第二直交关系求得。

类 元数 特征标	$C_1$	$C_2$	$C_3$	$C_4$	$C_5$
1	1	15	20	12	12
$\chi_{\rho_1}$	1	1	1	1	1
$\chi_{\rho_2}$	4	0	1	-1	-1
$\chi_{\rho_3}$	3	-1	0	$\frac{1-\sqrt{5}}{2}$	$\frac{1+\sqrt{5}}{2}$
$\chi_{\rho_4}$	3	-1	0	$\frac{1+\sqrt{5}}{2}$	$\frac{1-\sqrt{5}}{2}$
$\chi_{\rho_5}$	5	1	-1	0	0

### § 36 特征标间的各种关系

把阶为  $n$  的有限群  $G$  类分为共轭类  $C_1, \dots, C_q$ , 如果  $C_i$  的代表是  $a_i$ ,  $C_i$  中元的个数是  $n_i$ , 那末  $G$  具有  $q$  个既约表现类, 如果它的代表系是  $\rho_1, \dots, \rho_q$ , 命  $\sqrt{\frac{n_i}{n}} \chi_{\rho_i}(a_i) = \beta_{ii}$ , 那末  $(\beta_{ii})$  成为  $(q, q)$  型酉矩阵这已在 § 33 中叙述。又在  $\chi_{\rho_i}(a_i)$  或  $\beta_{ii}$  之间有下面各种关系。

(1) 假定对于  $x \in G$ ,  $f_x$  是在 § 29 中定义的  $A(G)$  中元 (即  $f_x(x) = 1$ ;  $x \neq y \Rightarrow f_x(y) = 0$ ), 对于各  $C_i$ , 命  $X_i = \sum_{x \in C_i} f_x (\in A(G))$

(在 § 29 命题 5 的意义下如果把  $x$  与  $f_x$  同样看待, 那就有  $X_i = \sum_{x \in C_i} x$ , 在以下的讨论中, 这方法考虑容易)。于是  $X_i \cdot X_j$  (作为  $A(G)$  中元的积) 成为  $\sum_{x \in G} \alpha_{ijk} x$  的形状, 这时  $\alpha_{ijk}$  显然是自然数或 0, 假定  $x \sim y$  ( $x, y$  共轭), 容易得知  $\alpha_{ijk} = \alpha_{ikj}$ , 所以

$$X_i \cdot X_j = \sum_{k=1}^q \alpha_{ijk} X_k. \quad (36.1)$$

这里  $\alpha_{ijk}$  是自然数或 0.

现在假定  $\rho_v$  的矩阵表现是  $P_v$ , 那末  $\sum_{x \in C_i} P_v(x) = T_{vi} \in \mathfrak{M}(d_v, \mathbb{C})$  ( $d_v$  是  $\rho_v$  的级数) 与  $P_v(y)$ ,  $y \in G$  中任何个可换。实际上, 当  $x$  在  $C_i$  中变动时, 因为  $yx$  与  $xy$  作为全体是取相同的元, 所以

$$P_v(y) T_{vi} = \sum_{x \in C_i} P_v(y) P_v(x) = \sum_{x \in C_i} P_v(yx) = \sum_{x \in C_i} P_v(xy) = T_{vi} P_v(y).$$

因此由 § 26 定理 3 的系 1 得  $T_{vi} = \tau_{vi} E_{d_v}$  ( $\tau_{vi} \neq 0$ ). 因为  $\chi_{\rho_v}(x) = SP_v(x)$ ,  $\chi_{\rho_v}$  是类函数, 所以

$$\sum_{x \in C_i} \chi_{\rho_v}(x) = n_i \chi_{\rho_v}(a_i) = d_v \tau_{vi}. \quad (36.2)$$

又因为  $P_v(xy) = P_v(x) P_v(y)$ , 所以由 (36.1) 得<sup>①</sup>

$$T_{vi} \cdot T_{vj} = \sum_{k=1}^q \alpha_{ijk} T_{vk},$$

因此

$$\tau_{vi} \cdot \tau_{vj} = \sum_{k=1}^q \alpha_{ijk} \tau_{vk}. \quad (36.3)$$

它由 (36.2) 能够直接重写为  $\chi_{\rho_v}(a_i)$  或  $\beta_{vi}$  間的关系。它是酉矩阵  $(\beta_{vi})$  中列之間的关系。

① 因为  $T_{vi} = \sum_{x \in C_i} P_v(x)$ , 由 (36.1) 及  $P_v(xy) = P_v(x) P_v(y)$ , 即得

$$T_{vi} T_{vj} = (P_v(x_1 + x_2 + \cdots + x_{n_i})) (P_v(y_1 + y_2 + \cdots + y_{n_j})),$$

其中

$$x_1 + x_2 + \cdots + x_{n_i} = C_i, \quad y_1 + y_2 + \cdots + y_{n_j} = C_j,$$

于是

$$T_{vi} T_{vj} = P_v[(x_1 + x_2 + \cdots + x_{n_i})(y_1 + y_2 + \cdots + y_{n_j})] = P_v(C_i C_j).$$

把  $f_x$  看成  $x$ , 由 (36.1) 得

$$T_{vi} T_{vj} = P_v \left[ \sum_{k=1}^q \alpha_{ijk} C_k \right] = \sum_{k=1}^q \alpha_{ijk} P_v(C_k) = \sum_{k=1}^q \alpha_{ijk} T_{vk}. \quad \text{——译者注}$$

由 (36.3), 又得知  $\tau_{\alpha}$  是  $(q, q)$  型矩陣  $(a_{ijk})_{j, k=1, \dots, q}$  的特征值。由这事实与  $a_{ijk} \in \mathbf{Z}$ , 根据数論的知識, 能够导出下面定理。

**定理 26** 有限群的既約表現的級数是它的阶数的約数。

在这定理的証明中, 代数整数的概念与它的简单性质都是需要的。又因为定理 26 是优美的定理, 对它的証明也有兴趣, 因此說得不免离正題稍远。茲叙述如下(自表現論的立場是不欢迎这样“离开正題”的証明, 但是其他簡短的証明至今还没有得到)。

首先是代数整数的定义, 最高次的系数是 1, 其他系数都  $\in \mathbf{Z}$  这样代数方程的根, 叫做代数整数。代数整数全体的集合用  $A$  表示。显然  $\mathbf{C} \supset A \supset \mathbf{Z}$ 。

**例 1**  $\mathbf{Z}$  中元的連乘根是代数整数, 例如  $\sqrt{2}, \sqrt{3}, \sqrt{-1}, \frac{-1 + \sqrt{-3}}{2}$  (1 的 3 乘根)  $\in A$ 。

**例 2** 假如  $\alpha \in A$ , 那末  $\bar{\alpha} \in A$ 。

[解] 因为把  $\alpha$  作为根的实系数代数方程也把  $\bar{\alpha}$  作为根 (参照 112 頁命题 57 的証明中后段), 所以显然成立。

**命题 16** 假定  $\xi$  是有理数并且是代数整数, 那末  $\xi \in \mathbf{Z}$  (因此  $\mathbf{Z}$  中元也叫做有理整数)。

**証明** 假定  $\xi^n + a_1 \xi^{n-1} + \dots + a_n = 0, a_i \in \mathbf{Z}$ , 并且  $\xi$  是有理数。有理数  $\xi$  能够写成  $\xi = \frac{b}{a}, a, b \in \mathbf{Z}, (a, b) = 1, a > 0$  的形状。这时証明  $a = 1$  即可。把  $\xi = \frac{b}{a}$  代入上方程去分母得

$$b^n + a_1 a b^{n-1} + \dots + a_n a^n = 0, \quad (36.4)$$

如果  $a \neq 1$ , 那就有  $p \mid a$  这样的质数  $p$ , 因为  $(a, b) = 1$ , 所以  $p \nmid b$ 。但由 (36.4) 得

$$b^n = -a(a_1 b^{n-1} + \dots + a_n a^{n-1}),$$

这右边能用  $p$  除尽, 而左边不能用  $p$  除尽, 由这不合理即得  $a = 1$ 。

**命题 17** 由  $\mathbf{Z}$  中元构成的正方矩陣的特征值是代数整数。

**证明** 假定  $a_{ij} \in \mathbb{Z}$ ,  $i, j = 1, \dots, r$ , 因为  $\mathbb{Z}$  成为环, 所以矩阵  $A = (a_{ij})$  的特征多项式  $\Phi_A(x)$  (74 页) 最高次的系数是 1, 其他系数是  $\mathbb{Z}$  中元 (参照 74 页例 3)。因此  $A$  的特征值, 即  $\Phi_A(x) = 0$  的根是代数整数。

**系** (36.3) 中  $\tau_{\alpha}$  是代数整数。

**命题 18** 代数整数的和, 差, 积又是代数整数。

**证明** 先证明  $\xi, \eta \in \mathbf{A} \Rightarrow \xi + \eta \in \mathbf{A}$ . 因为  $\xi, \eta \in \mathbf{A}$ , 所以有满足

$$\xi^n + a_1 \xi^{n-1} + \dots + a_n = 0, \quad (36.5)$$

$$\eta^m + b_1 \eta^{m-1} + \dots + b_m = 0 \quad (36.6)$$

的  $a_i, b_i \in \mathbb{Z}$ . 今对于  $\nu = 0, 1, \dots, n-1$ ;  $\mu = 0, 1, \dots, m-1$  作  $mn$  个积  $\xi^\nu \eta^\mu$ , 命  $\xi + \eta = \zeta$ , 那末对于  $\nu < n-1, \mu < m-1$ ,

$$\xi^\nu \eta^\mu \zeta = \xi^{\nu+1} \eta^\mu + \xi^\nu \eta^{\mu+1},$$

对于  $\nu = n-1, \mu < m-1$ , 用 (36.5),

$$\begin{aligned} \xi^{n-1} \eta^\mu \zeta &= \xi^n \eta^\mu + \xi^{n-1} \eta^{\mu+1} \\ &= -a_1 \xi^{n-1} \eta^\mu - \dots - a_n \eta^\mu + \xi^{n-1} \eta^{\mu+1}. \end{aligned}$$

因为对于  $\mu = m-1$  时也能够用 (36.6) 同样改写, 所以如果命 1,  $\xi, \eta, \xi\eta, \dots, \xi^{n-1}\eta^{m-1}$  这  $mn$  个积分别为 (任意的, 但依一定的顺序)  $\omega_1, \omega_2, \dots, \omega_l$  ( $l = mn$ ), 那末

$$\omega_i \zeta = \sum_{j=1}^l a_{ij} \omega_j$$

中  $a_{ij} \in \mathbb{Z}$ . 所以  $\zeta$  是由  $\mathbb{Z}$  中元构成的正方矩阵  $(a_{ij})$  的特征值<sup>①</sup>,

① 命  $F = (a_{ij})$ ,  $x = \begin{pmatrix} \omega_1 \\ \vdots \\ \omega_l \end{pmatrix}$ , 那末

$$Fx = (a_{ij}) \begin{pmatrix} \omega_1 \\ \vdots \\ \omega_l \end{pmatrix} = \begin{pmatrix} \sum_{j=1}^l a_{1j} \omega_j \\ \vdots \\ \sum_{j=1}^l a_{lj} \omega_j \end{pmatrix} = \begin{pmatrix} \omega_1 \zeta \\ \vdots \\ \omega_l \zeta \end{pmatrix} = \begin{pmatrix} \omega_1 \\ \vdots \\ \omega_l \end{pmatrix} \zeta.$$

即  $Fx = \zeta x$ , 所以  $\zeta$  是  $(a_{ij})$  的特征值。——译者注



由命題 17,  $\zeta \in A$ .

$\xi - \eta \in A$ ,  $\xi \eta \in A$  都能够完全同样証明。

系  $A$  成为  $C$  的子环。

例 3 有限群的任意特征标  $\chi$  所取的值是代数整数。

[解]  $\chi$  所取的值是 1 的連乘根的和(194 頁例 4)。因此由上例 1 与命題 18, 显然成立。

**定理 26 的証明** 由 201 頁 (33.2),  $\sum_{i=1}^q n_i \chi_{\rho_\nu}(a_i) \overline{\chi_{\rho_\nu}(a_i)} = n$ , 所以由 (36.2),  $\sum_{i=1}^q \tau_{\nu_i} \overline{\chi_{\rho_\nu}(a_i)} = \frac{n}{d_\nu}$ . 但由命題 17 系,  $\tau_{\nu_i} \in A$ , 又由例 3 及例 2,  $\overline{\chi_{\rho_\nu}(a_i)} \in A$ . 于是由命題 18,  $\frac{n}{d_\nu} \in A$ . 因为  $\frac{n}{d_\nu}$  是有理数, 所以由命題 16,  $\frac{n}{d_\nu} \in \mathbb{Z}$ , 即  $d_\nu | n$ .

例 4 在  $\mathfrak{S}_3, \mathfrak{S}_4, \mathfrak{S}_5$  中既約表現的級数都是阶数的約数。在  $d_\nu$  之間还有关

	$n$	$q$	$d_\nu$
$\mathfrak{S}_3$	6	3	1 1 2
$\mathfrak{S}_4$	24	5	1 1 2 3 3
$\mathfrak{S}_5$	60	5	1 3 3 4 5

系  $\sum_{\nu=1}^q d_\nu^2 = n$  (定理 17 系 1)。又  $d_\nu$  中至少有一个 (恒等表現的次数) 是 1, 这都是大家知道的。注意这事实与  $q$  分別是 3, 5, 5 的情况,  $d_\nu$  的值不可能在表中所示的以外, 这只要通过試行 (否则将导出

錯誤) 就容易明白。一般 (当  $n$  不太大时),  $d_\nu$  也能够这样求出。

例 5 因为在 (36.1) 中显然  $X_i X_j = X_j X_i$ , 所以  $a_{ijk} = a_{jik}$ . 又假如共軛类  $\{e_i\}$  用  $C_i$  表示, 对于  $C_i$ , 由  $C_i$  中元的逆元形成的共軛类 (因为  $x \sim y \Rightarrow x^{-1} \sim y^{-1}$ , 所以  $C_i$  中元的逆元作成一個共軛类) 用  $C_i'$  表示, 于是由 (36.1), 显然  $a_{ij1} = n_i \delta_{ij}$ ,  $a_{ijk} = a_{j1k} = \delta_{jk}$ . 又由結合律  $(X_i X_j) X_k = X_i (X_j X_k)$  即得

$$\sum_{k=1}^q a_{ijk} a_{ktm} = \sum_{k=1}^q a_{ikm} a_{jtk}.$$

(2) 命  $(\rho_\lambda \otimes \rho_\mu : \rho_\nu) = b_{\lambda\mu\nu}$ , 那末  $b_{\lambda\mu\nu}$  当然是自然数或 0,

$$\rho_\lambda \otimes \rho_\mu = \sum_{\nu=1}^q b_{\lambda\mu\nu} \rho_\nu.$$

因此由 195 頁命題 9(iv), 得到关于  $\chi_{\rho_\nu}(a_i)$  的关系

$$\chi_{\rho_\lambda}(a_i) \chi_{\rho_\mu}(a_i) = \sum_{\nu=1}^q b_{\lambda\mu\nu} \chi_{\rho_\nu}(a_i). \quad (36.7)$$

它是酉矩陣  $(\beta_{\lambda\mu})$  中行之間的关系。

**例 6** 假定  $\rho_1$  是恒等表現,  $\rho_v$  是  $\rho_v$  的反步表現, 在  $b_{\lambda\mu\nu}$  之間也与例 5 同样存在

$$b_{\lambda\mu\nu} = b_{\mu\lambda\nu}, \quad b_{1\mu\nu} = b_{\mu 1\nu} = \delta_{\mu\nu}, \quad b_{\lambda\mu 1} = \delta_{\lambda'\mu},$$

$$\sum_{\kappa=1}^q b_{\lambda\mu\kappa} b_{\kappa\nu\sigma} = \sum_{\kappa=1}^q b_{\lambda\kappa\sigma} b_{\mu\nu\kappa}.$$

証明也与例 5 的情况同样。

**例 7** 在  $\mathfrak{S}_3$  的情况中存在

$$\begin{aligned} \rho_1 \otimes \rho_v &= \rho_v \otimes \rho_1 = \rho_v \quad (v=1, 2, 3), \\ \rho_2 \otimes \rho_2 &= \rho_1, \quad \rho_2 \otimes \rho_3 = \rho_3 \otimes \rho_2 = \rho_3, \\ \rho_3 \otimes \rho_3 &= \rho_1 \oplus \rho_2 \oplus \rho_3. \end{aligned}$$

这里  $\rho_1, \rho_2, \rho_3$  是依照 202 頁例 5 的記法。

(3)  $d_v$  中等于 1 的个数由  $G$  的群构造确定, 有下面的定理 27。因为这定理需用“换位子”的概念来叙述, 所以, 首先应对此有所說明。

对于  $x, y \in G, xyx^{-1}y^{-1}$  是  $G$  中元, 它叫做  $x, y$  的换位子 (commutator), 用  $C(x, y)$  表示。  $C(x, y) = e$  是  $x, y$  为可換 ( $xy = yx$ ) 的必要充分条件。一般, 因为  $xy = C(x, y)yx$ , 所以  $C(x, y)$  可以考虑为表示  $x, y$  “不可換的程度”。

**例 8**  $C(x, y)C(y, x) = e, C(zxz^{-1}, zyz^{-1}) = zC(x, y)z^{-1}.$

$x, y$  在  $G$  中变动时, 用  $C(x, y)$  生成的  $G$  的子群叫做  $G$  的换位子群, 用  $G'$  表示。象在例 8 的第二式那样, 因为换位子  $C(x, y)$  的共轭元  $zC(x, y)z^{-1}$  是  $z x z^{-1}$  与  $z y z^{-1}$  的换位子, 所以  $G'$  是  $G$  的正規子群。

**命题 19**  $G/G'$  是可換群。又假如  $H$  是  $G$  的正規子群,  $G/H$  是可換, 那末  $H \supset G'$ 。

**証明** 因为  $xy = C(x, y)yx, C(x, y) \in G'$ , 所以  $xy \equiv yx \pmod{G'}$ , 因此  $G/G'$  是可換群。又假如  $G/H$  是可換群, 那末  $xy \equiv yx \pmod{H}$ 。

于是  $C(x, y) \in H$  对于所有的  $x, y \in G$  成立。所以  $G' \subset H$ 。

**定理 27** 在有限群  $G$  的既約表現中，級数  $d_\nu = 1$  的个数等于  $G$  中换位子群  $G'$  的指数  $(G:G')$ 。

**証明** 假定  $G$  的既約表現类的代表系  $\rho_1, \dots, \rho_q$  中  $\rho_\nu$ ,  $\nu = 1, \dots, k$  是 1 級，其他  $(q-k)$  个的級数  $\geq 2$ 。因为  $\rho_\nu(G)$ ,  $\nu = 1, \dots, k$  可換，所以由上命题， $\text{Ker } \rho_\nu \supset G'$ 。于是把  $G$  类分为  $G'$  的剩余类， $G = a_1 G' + \dots + a_m G'$  时，如果  $x \in a_i G'$ ，那末  $\rho_\nu(x) = \rho_\nu(a_i)$ 。假如由  $\bar{\rho}_\nu(a_i G') = \rho_\nu(a_i)$  定义  $\bar{\rho}_\nu: G/G' \rightarrow V$  ( $G$  的表現空間)，那末  $\bar{\rho}_\nu$  成为可換群  $G/G'$  的既約表現。反之，可換群  $G/G'$  的任意既約表現  $\bar{\rho}$  是 1 級的，它的核，取滿足  $G \supset H \supset G'$  的  $G$  的适当正規子群  $H$ ，表为  $H/G'$  形状。于是对于  $x \in G$ ，如果  $\rho(x) = \bar{\rho}(xG')$ ，那末  $\rho$  成为  $G$  的 1 級既約表現。因为  $G$  的 1 級既約表現  $\rho$  与  $G/G'$  的既約表現  $\bar{\rho}$  之間上面的对应显然是一对一的，所以两者的个数相等。因为  $G/G'$  是可換，所以它的个数等于  $G/G'$  的阶  $(G:G')$ 。

	$C_1$	$C_2$	$C_3$	$C_4$	$C_5$
$\chi_{\rho_1}$	1	1	1	1	1
$\chi_{\rho_2}$	1	1	1	-1	-1
$\chi_{\rho_3}$	1	1	-1	1	-1
$\chi_{\rho_4}$	1	1	-1	-1	1
$\chi_{\rho_5}$	2	-2	0	0	0

**例 9** 在四元数群  $Q = \{\pm 1, \pm i, \pm j, \pm k\}$  (§ 29 例 4)，因为  $iji^{-1}j^{-1} = -1$ ，所以  $Q$  的换位子群  $Q' = \{1, -1\}$  与中心一致是容易明白的。又共轭类是  $C_1 = \{1\}$ ,  $C_2 = \{-1\}$ ,  $C_3 = \{i, -i\}$ ,  $C_4 = \{j, -j\}$ ,  $C_5 = \{k, -k\}$  5 个。

$Q/Q' = \{Q', iQ', jQ', kQ'\}$ ，它显然与四元群 (§ 34 例 2) 同构。所以  $Q$  有 4 个 1 級既約表現  $\rho_1, \rho_2, \rho_3, \rho_4$ 。它的特征标(或表現自身)与四元群的相同。因为  $Q$  自身不是可換，所以第 5 个既約表現  $\rho_5$  的級数  $d_5 > 1$ 。但因为  $8 = 1^2 + 1^2 + 1^2 + 1^2 + 2^2$ ，所以不得不  $d_5 = 2$ 。 $\chi_{\rho_5}$  能够由特征标的第二直交关系求出。其結果如上。

(4) 假定  $\rho$  是  $n$  阶群  $G$  的  $d$  級既約表現， $G \ni x \rightarrow P(x)$  是  $\rho$  的矩陣表現。如果  $P(x) = (\alpha_{ij}(x))$ ，那末由定理 12 (191 頁)，

$$\begin{aligned}
\sum_{x \in G} \alpha_{ij}(ax) \alpha_{jl}(bx^{-1}) &= \sum_{x \in G} \left\{ \left( \sum_{k=1}^d \alpha_{ik}(a) \alpha_{kj}(x) \right) \left( \sum_{l=1}^d \alpha_{jl}(b) \alpha_{li}(x^{-1}) \right) \right\} \\
&= \sum_{k=1}^d \sum_{l=1}^d \left( \sum_{x \in G} \alpha_{kj}(x) \alpha_{li}(x^{-1}) \right) \alpha_{ik}(a) \alpha_{jl}(b) \\
&= \frac{n}{d} \alpha_{ii}(a) \alpha_{jj}(b).
\end{aligned}$$

把第二边与最右边就  $i, j=1, \dots, d$  相加, 再两边用  $d$  乘即得

$$d \sum_{x \in G} \chi_\rho(axbx^{-1}) = n \chi_\rho(a) \chi_\rho(b). \quad (36.8)$$

为了把这左边变形, 考虑  $b$  的正规化群  $N(b)$ . 把  $G$  类分为关于  $\text{mod } N(b)$  的左剩余类, 假定  $G = y_1 N(b) + \dots + y_m N(b)$ .  $m = (G:N(b))$  等于  $G$  中与  $b$  共轭的元的个数。与  $b$  共轭的元用  $b_1, \dots, b_m$  ( $b_1 = b$ ) 表示。又因为  $z \in N(b) \Leftrightarrow zbz^{-1} = b$ ,  $N(b)$  的阶  $= \frac{n}{m}$ , (36.8) 的左边能够变形如下:

$$\begin{aligned}
d \sum_{i=1}^m \sum_{z \in N(b)} \chi_\rho(ay_i z b z^{-1} y_i^{-1}) &= d \frac{n}{m} \sum_{i=1}^m \chi_\rho(ay_i b y_i^{-1}) \\
&= \frac{dn}{m} \sum_{i=1}^m \chi_\rho(ab_i).
\end{aligned}$$

因此, 由 (36.8) 得到下面的关系:

$$m \chi_\rho(a) \chi_\rho(b) = d \sum_{i=1}^m \chi_\rho(ab_i). \quad (36.9)$$

这是矩阵  $(\chi_{\rho_i}(a_i))$  或  $(\beta_{\nu i})$  中列之间的又一个关系。

以上是作为证明下面定理的准备。

**定理 28** 假定  $G$  是有限群,  $A(G)$  是它的群代数,  $C(A(G)) = U(G)$  是  $A(G)$  的中心, 即  $G$  的类函数的集合。那末  $\chi \in A(G)$  满足下面条件 (i) ~ (v), 是  $\chi$  成为  $G$  的单纯特征标的必要充分条件。

(i)  $\chi \in U(G)$ , (ii)  $(\chi, \chi) = 1$ , (iii)  $\chi(e) \in \mathbf{R}$ ,  $\chi(e) > 0$ .  
(iv)  $\chi(x^{-1}) = \overline{\chi(x)}$ .

(v) 假定  $a, b$  是  $G$  中任意两元,  $\{b_1, \dots, b_m\}$  是与  $b$  共轭元

全体的集合时,

$$m\chi(a)\chi(b) = \chi(e)(\chi(ab_1) + \cdots + \chi(ab_m)). \quad (36.10)$$

**证明** 这等条件是必要。假定  $\chi$  是  $G$  的某既约表现  $\rho$  的特征标  $\chi_\rho$ , 那末 (i), (ii), (iv) 成立, 已在 § 33, § 32 中明示。因为  $\chi(e) = (\rho \text{ 的级数})$ , 所以 (iii) 也是明显的。又 (v) 成立在上面已证明。

下面示 (i)~(v) 是充分的。再把  $\rho$  作为  $G$  的任意既约表现, 那末

$$m\chi_\rho(a)\chi_\rho(b) = \chi_\rho(e)(\chi_\rho(ab_1) + \cdots + \chi_\rho(ab_m)) \quad (36.10')$$

成立。把  $G$  类分为共轭类  $C_1, \cdots, C_q$ , 自各类  $C_i$  取代表  $b^{(i)}$ ,  $C_i$  中元的个数假定是  $n_i$ , 在 (36.10), 命  $b = b^{(i)}$ , 那末

$$n_i\chi(a)\chi(b^{(i)}) = \chi(e)(\chi(ab_1^{(i)}) + \cdots + \chi(ab_m^{(i)})).$$

在这式两边乘以  $\chi_\rho((b^{(i)})^{-1})$ , 就  $i=1, \cdots, q$  相加, 即得

$$n\chi(a)(\chi, \chi_\rho) = \chi(e)(\chi \cdot \chi_\rho(a)), \quad (36.11)$$

但  $(\chi, \chi_\rho)$  是在  $A(G)$  的内积 (§ 31),  $\chi \cdot \chi_\rho$  是  $A(G)$  中两元  $\chi, \chi_\rho$  的积 (§ 29)。在 (36.10') 中把  $\chi, \chi_\rho$  互换, 完全同样得到

$$n\chi_\rho(a)(\chi_\rho, \chi) = \chi_\rho(e)(\chi_\rho \cdot \chi)(a). \quad (36.11')$$

这里因为  $\chi \in C(G)$ , 所以  $\chi \cdot \chi_\rho = \chi_\rho \cdot \chi$ 。因此由 (36.11), (36.11') [用 (iii)] 得

$$\frac{\chi(a)}{\chi(e)}(\chi, \chi_\rho) = \frac{\chi_\rho(a)}{\chi_\rho(e)}(\chi_\rho, \chi).$$

但  $(\chi_\rho, \chi) = \frac{1}{n} \sum_{x \in G} \chi_\rho(x^{-1}) \overline{\chi(x^{-1})} = \frac{1}{n} \sum_{x \in G} \chi(x) \overline{\chi_\rho(x)} = (\chi, \chi_\rho)$ , 因此

$$\left( \frac{\chi(a)}{\chi(e)} - \frac{\chi_\rho(a)}{\chi_\rho(e)} \right) (\chi, \chi_\rho) = 0 \quad (36.12)$$

对于所有的  $a \in G$  成立。当  $\rho$  在既约表现的代表系  $\{\rho_1, \cdots, \rho_q\}$  上变动时, 因为  $\chi_\rho$  是  $C(G)$  的基底, 所以由 (i),

$$\chi = \sum_{i=1}^q \lambda_i \chi_{\rho_i},$$

因为  $(\chi_{\rho_i}, \chi_{\rho_j}) = \delta_{ij}$ , 所以  $(\chi, \chi) = \sum |\lambda_i|^2$ ,  $(\chi, \chi_{\rho_i}) = \lambda_i$ . 由 (ii)  $\lambda_i = (\chi, \chi_{\rho_i})$  中必定有不是 0 的。假定 (36.12) 中的  $\rho$  使  $(\chi, \chi_{\rho}) \neq 0$ , 那末

$$\frac{\chi(a)}{\chi(e)} = \frac{\chi_{\rho}(a)}{\chi_{\rho}(e)}$$

对于所有的  $a \in G$  成立, 即  $\chi = c\chi_{\rho}$  ( $c = \frac{\chi(e)}{\chi_{\rho}(e)}$ ), 但由 (ii),  $|c|^2 = 1$ , 更由 (iii) 不得不  $c = 1$ . (証毕)

关于构造简单的群, 利用定理 28——作为函数方程 (i) ~ (iv) 的解——能够求出单纯特征标。

#### 例 10 4 阶 2 面体群 $D_4$ .

一般在空间内有正  $n$  角形  $P_n$  时, 把  $P_n$  重合于它自身的空间运动形成的群叫做  $n$  阶 2 面体群 (dihedral group), 用  $D_n$  表示。假定  $P_n$  的平面是  $\alpha$ , 它的中心是  $O$ , 过  $O$  垂直  $\alpha$  的直线是  $l$ , 連結  $O$  与一个 (确定的) 顶点  $A$  的直线是  $m$ , 那末  $D_n$  能够由繞  $l$  旋轉  $\frac{2\pi}{n}$  的旋轉  $a$  与繞  $m$  旋轉  $\pi$  的旋轉  $b$  生成, 具有  $e, a, a^2, \dots, a^{n-1}, b, ab, \dots, a^{n-1}b$  这样的  $2n$  个元。在生成元之間  $a^n = e$ ,  $b^2 = e$ ,  $bab = a^{-1}$  关系成立 (这里譬如  $ab$  表示先施行运动  $b$ , 次施行运动  $a$  的结果)。

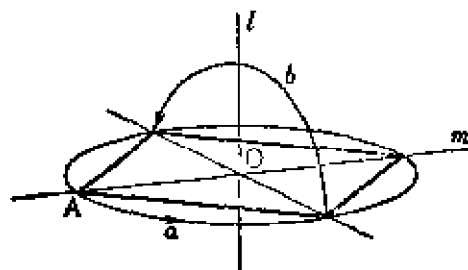


图 36.1

特别, 考虑  $D_4$  的情况。把  $D_4$  中八个元类分为共轭类成为  $C_1 = \{e\}$ ,  $C_2 = \{a^2\}$ ,  $C_3 = \{a, a^{-1} = a^3\}$ ,  $C_4 = \{b, a^2b = ba^2\}$ ,  $C_5 = \{ab = ba^{-1}, a^{-1}b = ba\}$  五个。 $\chi$  假定是单纯特征标, 因为这里各元与它的逆元属于同一共轭类, 由定理 28 (ii),

$$8(\chi, \chi) = \chi(e)^2 + \chi(a^2)^2 + 2(\chi(a)^2 + \chi(b)^2 + \chi(ab)^2) = 8 \quad (1)$$

成立。又命  $\chi(e) = d$ , 那末由 (iii),  $d > 0$ , 并且由 (v),

$$\begin{aligned} \chi(a^2)^2 &= d^2, \quad 2\chi(a)^2 = d(\chi(a^2) + d), \quad 2\chi(b)^2 = d(d + \chi(a^2)), \\ 2\chi(ab)^2 &= d(d + \chi(a^2)) \end{aligned} \quad (2)$$

成立。把它代入 (1),

$$2d^2 + 3d(d + \chi(a^2)) = 8, \quad (3)$$

由(2)的第一式,

$$\chi(a^2) = \pm d.$$

(i)  $\chi(a^2) = d$  时, 由(3),  $8d^2 = 8$ , 所以  $d = 1$ , 于是由(2),  $\chi(a)^2 = \chi(b)^2 = \chi(ab)^2 = 1$ , 并且  $\chi(a), \chi(b), \chi(ab)$  都等于  $\pm 1$ , 但再用(iv)得到

$\chi(a)\chi(b) = \chi(ab)$ ,  $\chi(b)\chi(ab) = \chi(a)$ ,  $\chi(ab)\chi(a) = \chi(b)$ , (4) 所以  $\chi(a), \chi(b), \chi(ab)$  中等于  $-1$  的必定是偶数个(0 或 2 个)。因此函数  $\chi$  是下表中  $\chi_1, \chi_2, \chi_3, \chi_4$  四个。

(ii)  $\chi(a^2) = -d$  时, 由(3),  $2d^2 = 8$ , 所以  $d = 2$ , 并且由(2)得  $\chi(a) = \chi(b) = \chi(ab) = 0$ , 它的解假定是  $\chi_5$ 。

	$C_1$	$C_2$	$C_3$	$C_4$	$C_5$
$\chi_1$	1	1	1	1	1
$\chi_2$	1	1	1	-1	-1
$\chi_3$	1	1	-1	1	-1
$\chi_4$	1	1	-1	-1	1
$\chi_5$	2	-2	0	0	0

而且, (1), (2), (4) 是  $D_4$  中单纯特征标满足的必要条件。但作为这等函数方程的解只得到  $\chi_1, \dots, \chi_5$  五个。并且因为单纯特征标的个数正好是 5, 所以它们给出所有的单纯特征标。

这特征标的表与在例 9 中所举的四元数群的特征标的表完全相同。但这两个群不同构。一般假定  $p$  是任意质数时

对于阶  $p^2$  的群同样事实成立是大家熟知的。

### § 37 群代数 $A(G)$ 的理想及幂等元

假定有限群  $G$  的共轭类的个数是  $q$ , 那末在  $G$  正好有  $q$  个既约表现类。如果它的代表系是  $\rho_1, \dots, \rho_q$ ,  $\rho_i$  的级数是  $d_i$ , 那末  $G$  的群代数  $A(G)$  与  $q$  个矩阵环的直和  $\mathfrak{M}(d_1, \mathbb{C}) \oplus \dots \oplus \mathfrak{M}(d_q, \mathbb{C})$  同构的事实在定理 19 已明示。在本节将引用这事实来研究作为  $G$  的表现空间的  $A(G)$  的构造。

假定  $f$  是  $A(G)$  中任意元, 那末  $S = A(G) \cdot f$  显然是  $A(G)$  的子空间, 并且

$$S \ni x, A(G) \ni a \Rightarrow ax \in S \quad (37.1)$$

成立。

一般对于代数  $R$  的子空间  $S$ ,

$$S \ni x, R \ni a \Rightarrow ax \in S \quad (37.2)$$

成立时,  $S$  叫做  $R$  的**左理想**①,

$$S \ni x, R \ni a \Rightarrow xa \in S \quad (37.3)$$

成立时,  $S$  叫做  $R$  的**右理想**。又

$$S \ni x, R \ni a \Rightarrow ax, xa \in S \quad (37.4)$$

成立时,  $S$  叫做  $R$  的**两侧理想**。(37.1) 表示  $A(G)f$  是  $A(G)$  的左理想。

**例 1** 假定  $f \in A(G)$ , 那末  $fA(G)$  是  $A(G)$  的右理想。又在上述自  $\mathfrak{M}(d_1, C) \oplus \cdots \oplus \mathfrak{M}(d_g, C)$  到  $A(G)$  的同构对应中,  $\mathfrak{M}(d_i, C)$  到  $A(G)$  中的象如果是  $A^{(i)}$ , 那末  $A^{(i)}$  是  $A(G)$  的两侧理想。

[解]  $fA(G)$  是  $A(G)$  的右理想是明显的。又证明  $A^{(i)}$  是  $A(G)$  的两侧理想时, 只要证明  $\mathfrak{M}(d_i, C)$  是  $\mathfrak{M}(d_1, C) \oplus \cdots \oplus \mathfrak{M}(d_g, C)$  的两侧理想即可。但这由矩阵的加法, 乘法的定义容易明白。

**例 2**  $S$  是  $R$  的两侧理想时, 对于  $a, b \in R$ , 定义

$$a \sim b \Leftrightarrow a \equiv b \pmod{S},$$

那末这“相合关系”是等价关系,

$$a \equiv b, a' \equiv b' \pmod{S} \Rightarrow a \pm a' \equiv b \pm b', aa' \equiv bb' \pmod{S}.$$

所以  $a, a'$  关于  $\text{mod } S$  的“相合类” $(a)_S, (a')_S$  之间由

$$(a)_S \pm (a')_S = (a \pm a')_S, (a)_S (a')_S = (aa')_S$$

能够引入和, 差, 积。这样就得到与  $R$  同态的代数  $R \text{ mod } S$ 。在这意义下, 代数的两侧理想是与群的正规子群相对应的。

象在 § 29 所叙述,  $A(G)$  是  $G$  的正则表现的表现空间,  $A(G)$  的左理想不外乎作为  $G$  的左正则表现的表现空间  $A(G)$  的不变子空间, 因而  $A(G)$  的左理想  $S$  又成为  $G$  的表现空间。当  $a \in G, f \in S$  时, 如果  $\rho(a)f = af \in S$ , 那末  $\rho$  是把  $S$  作为表现空间的  $G$  的左正则表现。

① “理想”(イデアール ideal) 为“理想子代数”之简称。——译者注



异于  $\{0\}$  的两侧理想除自身及  $\{0\}$  之外不再含两侧理想时,它叫做**最小两侧理想**。同样,异于  $\{0\}$  的左理想除自身及  $\{0\}$  之外不再含左理想时,叫做**最小左理想**。 $A(G)$  的最小左理想假如作为表现空间来看,不外是既约不变子空间,所以也叫做**既约左理想**。不是既约的左理想叫做**可约左理想**。关于右理想也是同样。

由定理 5 (171 页),  $G$  的任意表现空间  $V$  含其他表现空间  $V'$  时,存在满足  $V = V' \oplus V''$  这样的  $G$  的表现空间  $V''$ 。今假定  $V = A(G)$ , 那末对于  $A(G)$  的任意左理想  $S_1$ ,  $A(G)$  中有左理想  $S_2$  存在,使

$$A(G) = S_1 \oplus S_2. \quad (37.5)$$

因为  $A(G)$  有单位元  $e$ , 把它依 (37.5) 来分解, 假定  $e = e_1 + e_2$ ,  $e_i \in S_i$ , 那末对于  $A(G)$  中任意元  $f$  成为

$$f = f \cdot e = f e_1 + f e_2.$$

但因为  $S_i$  是左理想,  $e_i \in S_i$ , 所以  $f e_i \in S_i$ , 因此  $f e_i$  与把  $f$  依 (37.5) 分解时  $S_i$  的分量一致。特别, 如果  $f = e_1$ , 那末

$$e_1 = e_1 e_1 + e_1 e_2,$$

由分解的唯一性,  $e_1^2 = e_1$ ,  $e_1 e_2 = 0$ 。同样  $e_2^2 = e_2$ ,  $e_2 e_1 = 0$ 。一般环中元 2 乘不变的叫做**幂等元**。又环中两元  $x, y$  的积  $xy$  及  $yx$  都成为 0 时,  $x, y$  叫做**直交**。因此  $e_1, e_2$  是相互直交的幂等元。再假定  $f \in S_1$ , 那末  $f e_1 = f$ ,  $f e_2 = 0$ 。反之, 假定  $f e_1 = f$ , 显然  $f \in S_1$ 。由以上得到下面命题。

**命题 20**  $A(G)$  的任意左理想  $S$  有幂等元  $e$ , 并且能够写成  $S = A(G)e$  的形状。

**例 3** 0 是幂等元, 几个相互直交的幂等元的和又是幂等元。

**例 4** 在矩阵代数  $M(r, C)$  ( $C$  用任意体  $F$  来代替也可) 中,  $E_{ii}$  (只是第  $(i, i)$  元素是 1, 其他所有元素是 0 的矩阵) 是幂等元。假如  $i \neq j$ , 那末  $E_{ii}$  与

$E_{jj}$  是相互直交的幂等元。因此, 假如  $\delta_i$  是取 1 或 0 值的  $i$  的函数时,  $\delta_1 E_{11} + \delta_2 E_{22} + \cdots + \delta_r E_{rr}$  也是幂等元。

**例 5**  $A(G)$  的任意左理想能够分解为既约左理想的直和。

[解] 由定理 5 自明。

今假定  $A(G)$  的左理想  $S_0$  能够分解为几个左理想  $S_1, \cdots, S_r$  的直和:

$$S_0 = S_1 \oplus \cdots \oplus S_r. \quad (37.6)$$

把  $S_0$  的幂等元  $e_0$  依 (37.6) 分解, 命

$$e_0 = e_1 + \cdots + e_r, \quad (37.7)$$

那末  $e_i$  是  $S_i$  的幂等元, 并且当  $i \neq j$  时  $e_i, e_j$  是直交, 这与上面完全同样证明。

反之, 假如  $S_0$  中幂等元  $e_0$  是那样  $r$  个直交幂等元的和 ( $r \geq 2$ )  $e_1 + \cdots + e_r$ , 显然  $S_0 = A(G)e_0 = A(G)e_1 \oplus \cdots \oplus A(G)e_r$ .  $A(G)e_i = S_i$  是  $A(G)$  的左理想。因此, 假如  $S_0$  是既约理想, 那末  $S_0$  的幂等元  $e_0$  不能够分解为 (37.7) 的形状。能够分解为 (37.7) 那样直交幂等元的和的幂等元, 叫做可约的, 非 0 的幂等元不能够那样分解时, 叫做既约的。由这定义, 下面的命题显然成立。

**命题 21** 假如  $e_0$  是既约幂等元, 那末  $A(G)e_0$  是  $G$  的既约表现空间。假如  $e_0$  是可约幂等元, 那末  $A(G)e_0$  是  $G$  的可约表现空间。

由前面所述的事实及这命题得知, 求  $G$  的既约表现空间的问题归结于求  $A(G)$  中既约幂等元的问题。当  $e_0$  是既约幂等元时, 把  $A(G)e_0$  作为表现空间的既约表现  $\rho_0$  叫做“由幂等元  $e_0$  得到的表现”。反之, 既约表现  $\rho_0$  的表现空间  $A(G)$  中理想的幂等元  $e_0$  叫做“由表现  $\rho_0$  得到的幂等元”。又由两个既约幂等元  $e_1, e_2$  所得到的表现  $\rho_1, \rho_2$  是等价时, 幂等元  $e_1, e_2$  叫做等价, 用  $e_1 \sim e_2$  表示。

**命题 22** 假定  $e_i (i=1, 2)$  是  $A(G)$  的两个既约幂等元, 为了

$e_1 \sim e_2$ , 必要而充分的条件是  $A(G)$  中存在滿足  $e_1 f_1 e_2 \neq 0$  的元  $f_1$ .

**証明** 必要性. 假定由  $e_i$  得到的表現是  $\rho_i$ ,  $\rho_1 \sim \rho_2$  即假定自  $A(G)e_1$  到  $A(G)e_2$  作为表現空間的同构映射  $\varphi$  存在. 对于  $A(G)$

$$\begin{array}{ccc}
 A(G)e_1 & \xrightarrow{\rho_1(f)} & A(G)e_1 \\
 \varphi \downarrow & & \downarrow \varphi \\
 A(G)e_2 & \xrightarrow{\rho_2(f)} & A(G)e_2
 \end{array}
 \quad \text{并且} \quad \textcircled{1}$$

$g e_i \in A(G)e_i$ , 显然  $\rho_i(f) g e_i = f g e_i$ .  
 $f \varphi(g e_1) = \varphi(f g e_1)$ . (1)

今假定  $\varphi(e_1) = f_1$ , 在 (1) 如果命  $f = g = e_1$ , 那末  $e_1 f_1 = f_1$ . 因为  $e_1 \neq 0$ ,  $\varphi$  是同构映射, 所以  $f_1 \neq 0$ , 又因为  $f_1 \in A(G)e_2$ , 所以  $f_1 e_2 = f_1$ . 于是  $e_1 f_1 e_2 = f_1 \neq 0$ .

充分性. 假定  $e_1 f_1 e_2 = f_2 \neq 0$ , 对于  $A(G)e_1$  中元  $g e_1$ , 使  $g e_1 f_2$  对应的映射如果是  $\varphi$ . 因为  $g e_1 f_2 = (g e_1 f_1) e_2 \in A(G)e_2$ , 所以  $\varphi$  是自  $A(G)e_1$  到  $A(G)e_2$  的綫性映射, 显然 (1) 能够成立. 因此  $\varphi$  是自  $A(G)e_1$  到  $A(G)e_2$  的协变变换 (168 頁), 所以由 Schur 引理,  $\varphi = 0$  或  $\varphi$  是同构映射, 两者必居其一. 但因为  $\varphi(e_1) = f_2 \neq 0$ , 所以  $\varphi \neq 0$ . 因此  $\varphi$  不得不是同构映射.

**系 1** 假定  $a \in G$ , 如果  $e_2 = a e_1 a^{-1}$ , 那末  $e_1 \sim e_2$ .

**証明** 因为  $e_1 a^{-1} e_2 = e_1 a^{-1} \neq 0$ , 所以由上命題即得.

**系 2** 假如  $e_1 \sim e_2$  时,  $f$  是  $A(G)$  中滿足  $e_1 f e_2 \neq 0$  的元, 那末  $A(G)e_2 = (A(G)e_1) e_1 f e_2$ .

**証明** 由上命題的証明中能够推得.

**命題 23** 假定  $e_1 \sim e_2$ ,  $A(G)$  的兩側理想  $S$  含  $e_1$ , 那末  $S$  又含  $e_2$ .

**証明** 因为  $e_1 \in S$ ,  $S$  是左理想, 所以  $S \supset A(G)e_1$ . 又因为

① 如果把  $A(G)e_1 = V_1$ ,  $A(G)e_2 = V_2$  看成为  $A(G)$  的两个表現空間, 令  $g e_1 = V_1$ , 那末 (1) 式就是  $\rho_2(f)(\varphi(V_1)) = \varphi(\rho_1(f)V_1)$ . ——譯者注

$S$  是右理想, 所以  $S \supset (A(G)e_1)e_1fe_2$ . 于是由前命题的系 2,  $S \supset A(G)e_2$ . 因为  $A(G)$  具有单位元  $e$ , 所以  $S \ni e_2$ . (証毕)

在定理 19 的证明中, 给出自  $M(d_i, C)$  到  $A(G)$  中的同构映射, 即只在第  $j$  行第  $k$  列是 1, 其他元都是 0 这样的  $M(d_i, C)$  中元 ( $(d_i, d_i)$  型矩阵) 假定是  $E_{jk}^{(i)}$  时, 如果用 § 33 的记法, 使  $e_{jk}^{(i)}$  表示的  $A(G)$  中元与它对应就得到自  $M(d_i, C)$  到  $A(G)$  中的 ( $A^{(i)}$  上的) 同构对应  $\varphi_i$ . 由定理 18,  $d_i^2$  个元  $\{e_{jk}^{(i)}\}$  ( $j=1, \dots, d_i, k=1, \dots, d_i$ ) 构成  $A^{(i)}$  的基底, 由这对应这  $\sum_{i=1}^q d_i$  个  $e_{jk}^{(i)}$  是  $A(G)$  的既约幂等元,  $A(G)e_{jk}^{(i)}$  是  $A(G)$  的既约左理想. 这些都是明显的, 此外有下面的命题.

**命题 24**  $\{e_{1k}^{(1)}, \dots, e_{d_1k}^{(1)}\}$  是左理想  $A(G)e_{jk}^{(1)}$  的基底.

**证明**  $\{e_{1k}^{(1)}, \dots, e_{d_1k}^{(1)}\}$  是线性无关是明显的. 下面示明  $A(G)e_{jk}^{(1)}$  能够由它们生成即可. 假定

$$f \cdot e_{jk}^{(1)} \in A(G)e_{jk}^{(1)}, \quad f = \sum_{i=1}^q \sum_{\mu=1}^{d_i} \sum_{\nu=1}^{d_i} \lambda_{\mu\nu}^{(i)} e_{\mu\nu}^{(i)},$$

因为

$$f \cdot e_{jk}^{(1)} = \sum_{\mu=1}^{d_1} \sum_{\nu=1}^{d_1} \lambda_{\mu\nu}^{(1)} e_{\mu\nu}^{(1)} e_{jk}^{(1)} = \sum_{\mu=1}^{d_1} \sum_{\nu=1}^{d_1} \lambda_{\mu\nu}^{(1)} \delta_{\nu j} e_{\mu k}^{(1)} = \sum_{\mu=1}^{d_1} \lambda_{\mu j}^{(1)} e_{\mu k}^{(1)},$$

所以它是显然的. (証毕)

由这命题,  $A(G)e_{jk}^{(1)} = A(G)e_{jk}^{(1)}$ . 假如把它记成  $A_k^{(1)}$ , 那末  $A^{(1)} = A_1^{(1)} \oplus \dots \oplus A_{d_1}^{(1)}$ .

**系**  $A^{(i)}$  是  $d_i$  个  $d_i$  级既约左理想的直和.

把  $A^{(i)}$  分解为既约左理想的直和的方法虽然不是唯一的, 但由定理 6', 在任何分解中必定是  $d_i$  个  $d_i$  级左理想的直和, 这是明显的.

**例 6**  $e_{kk}^{(1)} \sim e_{kk'}^{(1)}$ , 因此  $A_k^{(1)} \sim A_{k'}^{(1)}$ .

**[解]** 因为  $e_{kk}^{(1)} e_{kk'}^{(1)} e_{kk'}^{(1)} = e_{kk'}^{(1)} \neq 0$ , 所以由命题 22, 得  $e_{kk}^{(1)} \sim e_{kk'}^{(1)}$ .

**例 7** 假定  $i \neq i'$ , 那末  $e_{kk}^{(i)} \not\sim e_{kk'}^{(i')}$ , 因此  $A_k^{(i)} \not\sim A_{k'}^{(i')}$ .

**[解]** 假定  $A(G) \ni f = \sum_{i=1}^q \sum_{\mu, \nu=1}^{d_i} \lambda_{\mu\nu}^{(i)} e_{\mu\nu}^{(i)}$ ,

那末 
$$e_{kk}^{(i)} f e_{k'k'}^{(i)} = \left( \sum_{\nu=1}^{d_i} \lambda_{k\nu} e_{k\nu}^{(i)} \right) e_{k'k'}^{(i)} = 0.$$

因此, 由命題 22,  $e_{kk}^{(i)} \not\sim e_{k'k'}^{(i)}$ .

**例 8** 假定  $e^{(i)} = \sum_{k=1}^{d_i} e_{kk}^{(i)}$ , 那末  $e^{(1)}, \dots, e^{(q)}$  是  $A(G)$  的直交幂等元,  $e = e^{(1)} + \dots + e^{(q)}$ . 又  $A^{(i)} \ni f \Leftrightarrow f = f e^{(i)} \Leftrightarrow f = e^{(i)} f \Leftrightarrow f = e^{(i)} f e^{(i)}$ . 因此  $A^{(i)} = A(G) e^{(i)} = e^{(i)} A(G) = e^{(i)} A(G) e^{(i)}$ .

[解] 后半段用  $e_{jk}^{(i)} e_{j'k'}^{(i)} = \delta_{ij} \delta_{kk'} e_{jk}^{(i)}$  容易推得.

**命題 25**  $A^{(i)}, i=1, \dots, q$ , 是  $A(G)$  的最小兩側理想.  $A(G)$  中最小兩側理想不外乎这  $q$  个  $A^{(i)}$ .

**証明** 在前半段, 如果  $A^{(i)}$  中异于  $\{0\}$  的任意兩側理想是  $S$  时, 示明  $S \ni e_{jk}^{(i)} (j, k=1, \dots, d_i)$  即可.

$S$  含非 0 的元  $f = \sum_{j,k=1}^{d_i} \lambda_{jk} e_{jk}^{(i)}$ . 今假定  $\lambda_{\mu\nu} \neq 0$ . 因为  $S$  是兩側理想, 所以  $S \ni \frac{1}{\lambda_{\mu\nu}} e_{\mu\nu}^{(i)} f e_{\mu\nu}^{(i)} = \frac{1}{\lambda_{\mu\nu}} \lambda_{\mu\nu} e_{11}^{(i)} = e_{11}^{(i)}$ . 于是由命題 23,  $e_{jj}^{(i)} \in S (j=1, \dots, d_i)$ , 因此, 又  $S \ni e_{jj}^{(i)} e_{jk}^{(i)} = e_{jk}^{(i)} (j, k=1, \dots, d_i)$ .

在証明后半段中, 假定  $A(G)$  的任意最小兩側理想是  $S$ , 如果  $A(G)$  中能够表为  $S \cdot A^{(i)}$  的有限个元的和的元全体的集合用  $[S \cdot A^{(i)}]$  表示, 显然  $[S \cdot A^{(i)}]$  又是  $A(G)$  的兩側理想. 并且显然  $[S \cdot A^{(i)}] \subset A^{(i)}$ , 所以由  $A^{(i)}$  的最小性,  $[S \cdot A^{(i)}] = \{0\}$  或  $A^{(i)}$ . 一方面, 因为  $A(G)$  含单位元  $e$ , 所以

$$\begin{aligned} S &= S \cdot A(G) = S(A^{(1)} \oplus \dots \oplus A^{(q)}) \\ &= S \cdot A^{(1)} \oplus \dots \oplus S \cdot A^{(q)} \subset [S \cdot A^{(1)}] + \dots + [S \cdot A^{(q)}]. \end{aligned}$$

因此  $[S \cdot A^{(i)}], i=1, \dots, q$ , 中至少有一个不是  $\{0\}$ . 对于这样的  $i, [S \cdot A^{(i)}] = A^{(i)}$ . 另一方面, 显然  $[S \cdot A^{(i)}] \subset S$ . 所以  $A^{(i)} \subset S$ , 因为  $A^{(i)}, S$  都同是最小兩側理想, 所以  $A^{(i)} = S$ . (証毕)

由命題 24 的系, 例 8 及命題 25 得出下面的定理.

**定理 29** 在群代数  $A(G)$  中有个数等于  $G$  的共軛类的个数  $q$  的最小兩側理想  $A^{(i)} (i=1, \dots, q)$ , 它們相互直交, 并且  $A(G)$

$= A^{(1)} + \cdots + A^{(q)}$ . 各最小两侧理想  $A^{(i)}$  能够分解为  $d_i$  个相互等价的  $d_i$  級既約左理想的直和。

**系**  $A(G)$  的任意两侧意队  $S$  是  $A^{(i)}$ ,  $i=1, 2, \cdots, q$  中几个的直和。

**証明** 因为  $A^{(i)}$  是最小两侧理想, 所以  $S \cap A^{(i)} = A^{(i)}$  或  $= \{0\}$  两者必居其一。今假定对于 (假如有必要就改变順序)  $i=1, 2, \cdots, p$ ,  $S \cap A^{(i)} = A^{(i)}$  (即  $S \supset A^{(i)}$ ), 对于  $j=p+1, \cdots, q$ ,  $S \cap A^{(j)} = \{0\}$  来証明  $S = A^{(1)} \oplus \cdots \oplus A^{(p)}$ . 因为由定理,  $A(G) = A^{(1)} \oplus \cdots \oplus A^{(q)}$ , 所以  $S$  中任意元  $x$  能够分解为  $x = x_1 + \cdots + x_q$ ,  $x_i \in A^{(i)}$  的形状, 这时只要証明  $x_j = 0$ ,  $j=p+1, \cdots, q$  即可。用例 8 的記法, 把  $A^{(j)}$  的幂等元写成  $e_j$ , 那末  $x_j = xe_j$ , 因为  $S, A^{(j)}$  是两侧理想, 所以  $xe_j \in S \cap A^{(j)} = \{0\}$ . 因此  $x_j = xe_j = 0$ .

**注意** 假如把  $A(G)$  考虑为  $G$  的左正则表現的表現空間, 那末  $A(G)$  的  $d_i$  級既約左理想不外于  $G$  的一个  $d_i$  級既約表現的表現空間。

### § 38 Young 的图形, 台与盘

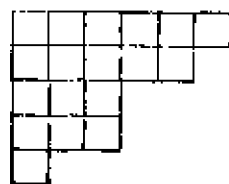
今后不再声明, 假定  $G = \mathfrak{S}_n = \mathfrak{S}(\{1, 2, \cdots, n\})$ . 象在 187 頁所述的那样,  $G$  的共轭类的个数  $q_n$  等于不定方程

$$n = m_1 + m_2 + \cdots + m_r, \quad m_1 \geq m_2 \geq \cdots \geq m_r > 0, \quad 1 \leq r \leq n \quad (38.1)$$

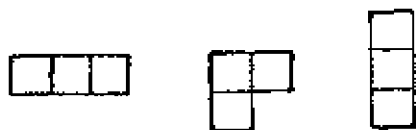
整数解的个数。并且对应于 (38.1) 的一个整数解的  $G$  的共轭类的代表能够取  $G$  的置換

$$(1, 2, \cdots, m_1) (m_1+1, \cdots, m_1+m_2) \cdots \\ \cdot (m_1+\cdots+m_{r-1}+1, \cdots, m_1+\cdots+m_r).$$

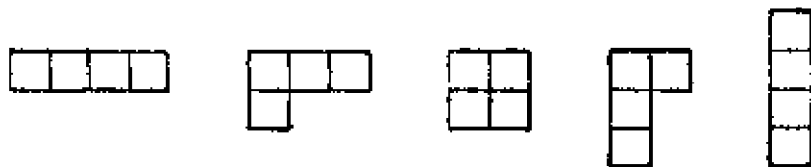
对于这共轭类 (或自然数  $n$  的分割), 使象右图那样, 持有第一行  $m_1$  个, 第二行  $m_2$  个,  $\cdots$ , 第  $r$  行  $m_r$  个“格子”的“ $n$  次台”对应。  $n$  次台应该有  $q_n$  个。



例1 3次台有



3个, 4次台有5个。



把数字  $1, 2, \dots, n$  排列在一个  $n$  次台的各个格子中所得的每一个图形, 叫做 **Young 图形**, 我们又简单地叫它做  $n$  次盘 (以下暂时假定  $n$  固定, 台和盘不再一一声明是“ $n$  次的”)。由一个台生成  $n!$  个盘。又台的“格子”有必要指示时, 象图中那样用“坐标”  $(i, j)$  表示。

$(1,1)$	$(1,2)$	$(1,3)$	...
$(2,1)$	$(2,2)$	$(2,3)$	...
$(3,1)$	$(3,2)$	$(3,3)$	...
$(4,1)$	$(4,2)$	$(4,3)$	...
...	...	...	...

再由一个台  $D$  生成的  $n!$  个盘的集合用  $\mathfrak{B}(D)$  表示。对于  $\mathfrak{B}(D)$  中元  $B$ , 假如施行  $G$  中元  $x = \begin{pmatrix} 1 & 2 & \dots & n \\ \nu_1 & \nu_2 & \dots & \nu_n \end{pmatrix}$ , 那就得到  $\mathfrak{B}(D)$  中另一元  $B'$ , 它用  $xB = B'$  表示。

所谓对于  $B$  “施行”  $x$  是下面的意义。例如, 假定

$$B = \begin{bmatrix} 3 & 2 \\ 1 \end{bmatrix}, x = (1 \ 2 \ 3), \text{ 那末 } xB = \begin{bmatrix} 1 & 3 \\ 2 \end{bmatrix}$$

一般, 假定  $B, B'$  的  $(i, j)$  格子中数字分别用  $B(i, j), B'(i, j)$  表示,

$$xB = B' \Leftrightarrow xB(i, j) = B'(i, j).$$

这时当然  $(xy)B = x(yB), eB = B, xB = B' \Leftrightarrow B = x^{-1}B'$ . 又假如取同一台上的两个盘  $B, B'$ , 显然存在成为  $B' = xB$  这样的  $x \in G$ .

**命题 26**  $xB = B \Leftrightarrow x = e$ .

**证明**  $xB = B$  意味着对于所有的  $n$  个  $(i, j)$ ,  $xB(i, j) = B(i, j)$ , 它意味着  $x = \begin{pmatrix} B(i, j) \\ B(i, j) \end{pmatrix} = e$ .

**系**  $xB = yB \Leftrightarrow x = y$ .

对于一个盘  $B$ ,  $G$  的元中把  $B$  的各行中元只在它的行中变动的叫做  $B$  的水平置换, 把  $B$  的各列中元只在它的列中变动的, 叫做  $B$  的垂直置换. 水平置换的全体, 垂直置换的全体显然分别成为  $G$  的子群. 它分别用  $\mathfrak{S}(B)$ ,  $\mathfrak{R}(B)$  表示. 显然  $G$  能够由  $\mathfrak{S}(B)$  与  $\mathfrak{R}(B)$  生成,  $\mathfrak{S}(B) \cap \mathfrak{R}(B) = \{e\}$ .  $\mathfrak{S}(B)$  的阶是  $m_1! m_2! \cdots m_r!$ .

**命题 27** 假如  $G \ni x = hk = h'k'$ , 或  $x = kh = k'h'$ ,  $h, h' \in \mathfrak{S}(B)$ ,  $k, k' \in \mathfrak{R}(B)$ , 那末  $h = h'$ ,  $k = k'$ .

**证明** 假定  $x = hk = h'k'$ , 那末  $h'^{-1}h = k'k^{-1} \in \mathfrak{S}(B) \cap \mathfrak{R}(B)$ . 所以  $h'^{-1}h = k'k^{-1} = e$ , 即  $h = h'$ ,  $k = k'$ . 当  $x = kh = k'h'$  时也同样. (证毕)

$G$  中各元  $x$  在 § 29 中  $f_x$  的意义下能够看成为  $A(G)$  中元. 于是一个盘  $B$  给定时, 由  $B$  得定义下面三个  $A(G)$  中元

$$\begin{aligned} H_B &= \sum_{h \in \mathfrak{S}(B)} h, & K_B &= \sum_{k \in \mathfrak{R}(B)} (\text{sgn } k) k, \\ c_B &= H_B K_B = \sum_{\substack{h \in \mathfrak{S}(B) \\ k \in \mathfrak{R}(B)}} (\text{sgn } k) hk. \end{aligned} \quad (38.2)$$

但  $\text{sgn } k$  是在  $k$  为偶置换时规定为 1,  $k$  为奇置换时规定为  $-1$  的  $k \in \mathfrak{R}(B)$  的函数. 当  $B$  给定而不致发生误解时,  $H_B, K_B, c_B$  分别简单写成  $H, K, c$ . 因为它们都是  $A(G)$  中元, 所以是  $G$  中元  $x$  的 (复数值) 函数. 例如  $c = c(x)$ .

由命题 27,  $x \in G$  写成  $x = hk$  ( $h \in \mathfrak{S}(B)$ ,  $k \in \mathfrak{R}(B)$ ) 形状时, 这种写法是唯一的. 假如  $x$  能够写成这形状, 由 (38.2),  $c(x) = \text{sgn } x$ . 假如  $x$  不能写成这形状,  $c(x) = 0$ , 即



$$c(x) = \begin{cases} \operatorname{sgn} k, & x = hk, \\ 0, & x \neq hk, \end{cases} \quad (38.3)$$

$c=c_B$  叫做由  $B$  确定的 **Young 的对称子** (Young symmetrizer)。这是 Alfred Young 在 1901 年 Proc. London Math. Soc. 上的論文中引入的。象在后面所示,  $c$  的某常数倍  $\frac{1}{\alpha} c$  ( $\alpha$  是自然数) 成为  $A(G)$  的既約幂等元。又  $A(G)$  的任意既約幂等元能够用  $\frac{1}{\alpha} c_B$  的形状給出 (这事实 Young 已証明, 但 Frobenius 在 1900 年的論文中早已証明同样事实)。

**例 2**  $n=3$ ,  $B = \begin{bmatrix} 1 & 2 \\ 3 \end{bmatrix}$  时,  $\mathfrak{S}(B) = \{1, (1, 2)\}$ ,  $\mathfrak{R}(B) = \{1, (1, 3)\}$ ,  $H = 1 + (1, 2)$ ,  $K = 1 - (1, 3)$ ,  $c = 1 + (1, 2) - (1, 3) - (1, 3, 2)$ 。

**命題 28**  $B' = xB$  时, 假如命  $\mathfrak{S}(B) = \mathfrak{S}$ ,  $\mathfrak{S}(B') = \mathfrak{S}'$ ,  $\mathfrak{R}(B) = \mathfrak{R}$ ,  $\mathfrak{R}(B') = \mathfrak{R}'$ ,  $H_B = H$ ,  $H_{B'} = H'$ ,  $K_B = K$ ,  $K_{B'} = K'$ ,  $c_B = c$ ,  $c_{B'} = c'$ , 那末

- (1)  $x\mathfrak{S}x^{-1} = \mathfrak{S}'$ ,  $x\mathfrak{R}x^{-1} = \mathfrak{R}'$ ,
- (2)  $xHx^{-1} = H'$ ,  $xKx^{-1} = K'$ ,  $xcx^{-1} = c'$ 。

**証明** 一般, 对于  $x, y \in G$ , 命  $xyx^{-1} = y'$ , 那末  $xy = y'x$ 。又假如  $h \in \mathfrak{S}$ , 那末  $hB(i, j) = B(i, j')$ 。因此  $xhB(i, j) = xB(i, j')$ 。命  $xh = h'x$ , 那末  $h'xB(i, j) = xB(i, j')$ 。即  $h' \in \mathfrak{S}'$ 。所以  $x\mathfrak{S}x^{-1} \subset \mathfrak{S}'$ 。同样,  $x^{-1}\mathfrak{S}'x \subset \mathfrak{S}$ 。于是  $x\mathfrak{S}x^{-1} = \mathfrak{S}'$ 。关于  $\mathfrak{R}$  也是同样。因此得到 (1)。 (2) 由它立即明白。

**例 3**  $B = \begin{bmatrix} 1 & 2 \\ 3 \end{bmatrix}$ ,  $B' = (1, 2, 3)B = \begin{bmatrix} 2 & 3 \\ 1 \end{bmatrix}$  时,  $H = 1 + (1, 2)$ ,  $K = 1 - (1, 3)$ ,

$$(1, 2, 3)H(1, 2, 3)^{-1} = (1, 2, 3)(1 + (1, 2))(1, 3, 2) = 1 + (2, 3) = H',$$

$$(1, 2, 3)K(1, 2, 3)^{-1} = (1, 2, 3)(1 - (1, 3))(1, 3, 2) = 1 - (1, 2) = K'.$$

**命題 29** 盘  $hB$  能够由首先把  $B$  中数字水平移动作成  $hB$ 。

再把盘  $hB$  中数字垂直移动得出。

**证明** 由  $hk = hkh^{-1}h$ , 并且  $hkh^{-1} \in \mathfrak{S}(hB)$  即得。

**注意** 因为  $h$  不一定是  $\mathfrak{S}(kB)$  中元, 所以  $hkB$  不能由先把  $B$  中数字垂直移动, 再把所得的盘中数字水平移动得出。

**命题 30** 对于  $x \in G$  能够写成  $x = hk$ ,  $h \in \mathfrak{S}(B)$ ,  $k \in \mathfrak{S}(B)$  的必要充分条件是  $B$  中在同行的两个数字在  $xB$  中不是在同列。

**证明** 必要性。假如  $x = hk$ , 那末  $xB$  能够自把  $B$  中数字首先水平移动, 再垂直移动得出。因此  $B$  中在同行的两个数字在  $xB$  中就在异列。

充分性。命  $B' = xB$ , 那末对于各对  $(i, j)$  成为  $B(i, j) = B'(l, p)$  这样的  $l = l(i, j)$ ,  $p = p(i, j)$  唯一确定。假如  $j_1 \neq j_2$ , 那末  $p(i, j_1) \neq p(i, j_2)$ 。因此  $B$  中各数字  $B(i, j)$  能够移于格子  $(i, p(i, j))$ , 这置换是水平置换。如果命它为  $h$ , 因为在  $hB$  与  $B'$  中同数字必定在同列, 由  $k' \in \mathfrak{S}(hB)$  能够使  $k'(hB) = B'$ , 即  $x = k'h$ 。于是, 如果命  $k = h^{-1}k'h$ , 那末由命题 28,  $k \in \mathfrak{S}(h^{-1}hB) = \mathfrak{S}(B)$ 。因此  $x = k'h = hkh^{-1}h = hk$ ,  $h \in \mathfrak{S}(B)$ ,  $k \in \mathfrak{S}(B)$ 。(证毕)

在两个盘  $B, B'$  中, 把“ $B$  中在同行的两个数字在  $B'$  中不在同列”这事实, 今后为了简单用  $B > B'$  或  $B' < B$  来表示。于是命题 30 能够表为“ $x = hk, h \in \mathfrak{S}(B), k \in \mathfrak{S}(B) \Leftrightarrow B > xB$ ”,  $B > B'$  的否定, 即“取适当的两数字, 它们在  $B$  中是在同行, 在  $B'$  中又是在同列,”这事实用  $B \nless B'$  或  $B' \nless B$  表示。假如  $B = B'$ , 那末  $B > B'$ , 但  $B > B'$ , 而  $B \neq B'$ , 用  $B \gg B'$  表示。

**命题 31** 假定  $xB = B'$ , 如果  $B \nless B'$ , 那就存在适当的对换  $h, k$ , 使  $hx = xk$ ,  $h \in \mathfrak{S}(B)$ ,  $k \in \mathfrak{S}(B)$  成立。

**证明** 假定在盘  $B$  属于同行, 在盘  $B'$  属于同列的两个数字是  $\mu, \nu$ 。命  $h = (\mu, \nu)$  (把  $\mu$  与  $\nu$  互换的对换), 显然  $h \in \mathfrak{S}(B)$ ,  $h \in \mathfrak{S}(xB)$ 。又命  $k = x^{-1}hx$ , 那末  $k$  也是对换,  $k \in \mathfrak{S}(x^{-1}xB)$

$$= \mathfrak{R}(B), \quad hx = xk.$$

系 当  $x \in G$  不能写成  $x = hk$ ,  $h \in \mathfrak{S}(B)$ ,  $k \in \mathfrak{R}(B)$  形状时, 存在适当的对换  $h', k'$  使  $h'x = xk'$ ,  $h' \in \mathfrak{S}(B)$ ,  $k' \in \mathfrak{R}(B)$  成立

**命题 32** (1)  $hH = Hh = H$ . (2)  $kK = Kk = (\text{sgn } k)K$ . (3) 对于任意  $h \in \mathfrak{S}, k \in \mathfrak{R}$ ,  $hck = (\text{sgn } k)c$ .

**证明** (1) 因为  $\mathfrak{S}$  是有限群, 故  $h\mathfrak{S} = \mathfrak{S}h = \mathfrak{S}$ , 由这显然成立.

$$(2) \quad kK = \sum_{k' \in \mathfrak{R}} (\text{sgn } k')kk' = (\text{sgn } k) \sum_{k' \in \mathfrak{R}} (\text{sgn } kk')kk' = (\text{sgn } k)K.$$

同样,  $Kk = (\text{sgn } k)K$ .

$$(3) \quad hck = hHKk = (\text{sgn } k)HK = (\text{sgn } k)c.$$

**命题 33** 对于任意  $h \in \mathfrak{S}(B)$ ,  $k \in \mathfrak{R}(B)$ , 假定  $f \in A(G)$  满足  $hfk = (\text{sgn } k)f$ , 那就存在  $\lambda \in \mathbb{C}$ , 使  $f = \lambda c$ .

**证明** 对于任意  $x \in G$ , 证明

$$f(x) = \begin{cases} \lambda (\text{sgn } k), & x = hk \\ 0, & x \neq hk \end{cases}$$

即可。由假定, 对于任意  $h \in \mathfrak{S}(B)$ ,  $k \in \mathfrak{R}(B)$ ,  $y \in G$ ,

$$(\text{sgn } k)f(y) = (h^{-1}fk^{-1})(y) = f(hyk) \text{ ①},$$

① 由假定  $h \in \mathfrak{S}(B)$ ,  $k \in \mathfrak{R}(B)$  时下式恒成立:

$$hfk = (\text{sgn } k)f,$$

此时有  $h^{-1} \in \mathfrak{S}(B)$  及  $k^{-1} \in \mathfrak{R}(B)$ , 因此下式也同样成立:

$$h^{-1}fk^{-1} = (\text{sgn } k^{-1})f.$$

因为  $\text{sgn } k = \text{sgn } k^{-1}$ , 所以

$$(\text{sgn } k)f = h^{-1}fk^{-1}.$$

将  $h^{-1}$ ,  $k^{-1}$  记为函数符号  $f_{h^{-1}}$  及  $f_{k^{-1}}$ , 则上式为

$$(\text{sgn } k)f = (f_{h^{-1}} \cdot f \cdot f_{k^{-1}})(y).$$

根据  $A(G)$  中元乘法定义,

$$\begin{aligned} (f_{h^{-1}} \cdot f \cdot f_{k^{-1}})(y) &= \sum_{x \in G} f_{h^{-1}}(y \cdot x^{-1}) (f \cdot f_{k^{-1}})(x) \\ &= \sum_{x \in G} f_{h^{-1}}(y \cdot x^{-1}) \sum_{z \in G} f(xz^{-1}) \cdot f_{k^{-1}}(z). \end{aligned}$$

上式右边只是当  $z = k^{-1}$ ,  $yx^{-1} = k^{-1}$  时不为 0, 其值等于  $f$  在  $hyk$  的值, 所以

$$(f_{h^{-1}} \cdot f \cdot f_{k^{-1}})(y) = f(hyk),$$

因此  $(\text{sgn } k)f(y) = f(hyk)$ . ——译者注

命  $f(e) = \lambda$ , 因为  $x = hkb$ , 所以  $f(x) = \lambda(\operatorname{sgn} k)$ . 又假如  $x \neq hkb$ , 由命题 31 的系,  $h'x = xk'$ , 因为  $\operatorname{sgn} k' = -1$ , 所以  $f(x) = f(h'^{-1}xk') = (\operatorname{sgn} k')f(x) = -f(x)$ , 因此  $f(x) = 0$ .

**命题 34** 对于任意  $f \in A(G)$ , 存在  $\mu \in C$ , 使  $cf c = \mu c$ .

**证明** 对于任意  $h \in \mathfrak{S}(B)$ ,  $k \in \mathfrak{R}(B)$  有  $h(cf c)k = hHKfHKk = (\operatorname{sgn} k)HKfHK = (\operatorname{sgn} k)cf c$ . 因此由前命题,  $cf c = \mu c$ ,  $\mu \in C$ .

**系** 存在使  $c^2 = \alpha c$  的  $\alpha \in Z$ .

**证明** 假定  $\alpha \in C$ , 由命题 34, 上式成立是明显的<sup>①</sup>. 因为  $c = \sum_{x=hk} (\operatorname{sgn} k) x$ , 所以  $c^2$  中  $x$  的系数是  $\sum (\operatorname{sgn} k)(\operatorname{sgn} k')$  形状的数字  $\in Z$ . 但  $c$  中  $x$  的系数是  $\pm 1$ , 所以存在满足  $c^2 = \alpha c$  的  $\alpha \in Z$ .

**命题 35**  $A(G)c$  是  $A(G)$  的左理想. 假如它的级数是  $d$ , 那末  $\alpha d = n!$  ( $n!$  是  $G$  的阶).

**证明** 显然  $A(G)c$  是  $A(G)$  的左理想.

其次, 假定由  $\tau(f) = fc$ ,  $f \in A(G)$ , 定义  $\tau: A(G) \rightarrow A(G)c$ , 那末  $\tau \in \mathfrak{L}(A(G))$ . 今假定  $A(G)$  的基底是  $\{a_1, \dots, a_n\}$ , 取<sup>②</sup>  $a_i \in A(G)c$ ,  $1 \leq i \leq d$ , 如果由这基底把  $\tau$  用矩阵表现, 因为

$$\tau(fc) = fc^2 = \alpha fc,$$

那就成为

形状. 因此  $\tau$  的迹  $S(\tau) = \alpha d$ .

① 假定  $f=e$ , 由命题 34 显然存在  $\alpha \in C$  使  $c^2 = \alpha c$  成立. ——译者注

② 即是说在  $\{a_1, \dots, a_n\}$  中, 特别取  $a_i \in A(G)c$ ,  $1 \leq i \leq d$ . ——译者注

一方取  $G$  中元作为  $A(G)$  的基底, 如果由这基底把  $\tau$  用矩陣表現, 那末它的对角綫上元素是  $xc \in A(G)$  在  $x$  的值  $(xc)(x)$ . 因为

$$(xc)(x) = \sum_y x(xy^{-1})c(y) = c(e) = 1,$$

它等于 1, 所以  $S(\tau) = n!$ . 因此

$$ad = n!.$$

系  $\alpha$  是自然数, 是  $n!$  的約数。

**命题 36** 假定  $\varepsilon = \frac{1}{\alpha} \cdot c = \frac{d}{n!} \cdot c$ , 那末  $\varepsilon$  是  $A(G)$  的既約幂等元。

**証明**  $\varepsilon^2 = \frac{1}{\alpha^2} \cdot c^2 = \frac{\alpha}{\alpha^2} \cdot c = \frac{1}{\alpha} \cdot c = \varepsilon.$

又假如  $\varepsilon = \varepsilon_1 + \varepsilon_2$ ,  $\varepsilon_1^2 = \varepsilon_1$ ,  $\varepsilon_2^2 = \varepsilon_2$ ,  $\varepsilon_1 \varepsilon_2 = \varepsilon_2 \varepsilon_1 = 0$ , 那末  $\varepsilon \varepsilon_1 \varepsilon = (\varepsilon_1 + \varepsilon_2) \varepsilon_1 (\varepsilon_1 + \varepsilon_2) = \varepsilon_1$ . 但由命题 34, 它等于  $\mu' \varepsilon (\mu' \in C)$ . 所以  $\varepsilon_1 = \mu' \varepsilon$ . 于是  $\varepsilon_1^2 = \mu'^2 \varepsilon$ . 因为  $\varepsilon_1^2 = \varepsilon_1$ , 所以  $\mu' = 1$  或 0. 这意味着  $\varepsilon = \varepsilon_1$  或  $\varepsilon = \varepsilon_2$ . (証毕)

这样, 由一个盘  $B$  就得到一个  $A(G)$  的既約幂等元  $\varepsilon$ , 因而得到一个把  $A(G)\varepsilon$  作为表現空間的  $G$  的既約表現。但是象在定理 30 叙述的那样, 由属于相同台的盘所得到的既約表現相互等价, 由属于相异台的盘所得到的既約表現是不等价。因为台的个数是与  $G$  的共轭类的个数  $q$  相同, 所以上面那样  $q$  个相互不等价的既約表現已經是全部的了。这些結論順次証明于下。

**命题 37** 自属于同一台的两个盘  $B, B'$  象上面那样得到的既約幂等元是相互等价的。

**証明** 假定  $B, B'$  属于同一台, 那末存在使  $B' = xB$  的  $x \in G$ . 于是由命题 28,  $c' = xcx^{-1}$ , 因此  $\varepsilon' = x\varepsilon x^{-1}$ , 所以  $\varepsilon$  与  $\varepsilon'$  等价。

(証毕)

其次, 为了考虑自相异台得到的幂等元, 在台的集合  $\{D\}$  中, 給定下面那样的順序。假定确定  $D, D'$  的不变系分別是  $(m_1, m_2, \dots,$

$m_r)$ ,  $(m'_1, m'_2, \dots, m'_r)$ , 如果  $m_1 = m'_1, \dots, m_\nu = m'_\nu, m_{\nu+1} > m'_{\nu+1}$ , 那就规定  $D > D'$ . 假定  $D > D'$  或  $D = D'$  表为  $D \geq D'$ , 那末由  $\geq$ ,  $\{D\}$  就成为全序集 (154 页)。

**命题 38** 假定盘  $B, B'$  分别属于台  $D, D'$ , 如果  $D > D'$ , 那末  $B \succ B'$ .

**证明** 假定  $B \succ B'$  并且  $B$  中第一行的  $m_1$  个数字都在  $B'$  的异列, 那末  $B'$  的列数超过  $m_1$ , 因此  $m'_1 \geq m_1$ . 一方, 因为  $D > D'$ , 所以  $m_1 \geq m'_1$ . 于是  $m_1 = m'_1$ . 因此对  $B'$  施行适当的垂直置换  $k$ , 能够使得  $B$  中第一行的  $m_1$  个数字落在  $kB'$  中第一行。这时  $B$  中在同一行的数字都落在  $kB'$  中的异列。因为  $m_1 = m'_1$ , 再比较  $B$  与  $kB'$  的第二行, 同样  $m_2 = m'_2$ . 以下同样做得到  $m_i = m'_i, i = 1, 2, \dots, r$ , 这与  $D > D'$  相反。

**命题 39** 假定  $B \succ B'$ , 那末  $HK' = K'H = 0, \varepsilon'\varepsilon = 0$ .

**证明** 因为存在满足  $h = (\mu, \nu) \in \mathfrak{S}(B) \cap \mathfrak{S}(B')$  的数字  $\mu, \nu$ , 所以由命题 32,  $HK' = HhK' = (\text{sgn } h)HK' = -HK'$ . 因此  $HK' = 0$ . 同样  $K'H = 0$ , 所以  $\varepsilon'\varepsilon = \frac{1}{\alpha\alpha'} H'K'HK = 0$ .

**注意**  $\varepsilon\varepsilon' = 0$  不一定成立。

**命题 40** 假定  $D > D'$ ,  $B, B'$  是属于台  $D, D'$  的任意盘, 如果  $\varepsilon = \varepsilon_B, \varepsilon' = \varepsilon_{B'}$ , 那末对于任意的  $f \in A(G)$ ,

$$\varepsilon'f\varepsilon = 0.$$

**证明** 对于任意  $x \in G, xB \in \mathfrak{B}(D), B' \in \mathfrak{B}(D')$ , 因为  $D > D'$ , 由命题 38, 39,  $\varepsilon'\varepsilon_{xB} = 0$ . 但  $\varepsilon_{xB} = x\varepsilon x^{-1}$ . 所以  $\varepsilon'x\varepsilon x^{-1} = 0$ . 再把  $x$  右乘得  $\varepsilon'xe = 0$ . 它对于所有的  $x \in G$  成立。因此

$$\varepsilon'f\varepsilon = \sum_{x \in G} f(x) \varepsilon'xe = 0. \quad (\text{证毕})$$

由这命题及命题 22 得知, 自  $B, B'$  得到的既约表现不等价。

总结以上, 利用 Young 的图形得到下面解决全部求  $G = \mathfrak{S}_n$

的既約表現問題的定理。

**定理 80** 假定  $G$  是  $n$  阶对称群,  $B, B'$  是  $n$  次盘。

(1) 假如  $B$  的 Young 的对称子是  $e$ , 那末  $A(G)e$  成为  $G$  的既約表現的表現空間。

(2) 自盘  $B$ , 盘  $B'$  得到的  $G$  的既約表現是等价的必要充分条件是  $B$  与  $B'$  属于同台。

(3)  $G$  的任意既約表現是与自某盘  $B$  象 (1) 那样得到的既約表現等价。

例 4

自台  $D^{(1)} = \begin{array}{|c|c|c|c|} \hline & & & \\ \hline \end{array}$ , 台  $D^{(2)} = \begin{array}{|c|} \hline \\ \hline \vdots \\ \hline \end{array}$  得到的既約表現分別是恒等表現, 交代表現。

[解] 假定取属于  $D^{(1)}$  的任意盘  $B_1$ , 那末  $\mathfrak{S}(B_1) = G$ ,  $\mathfrak{N}(B_1) = \{e\}$ . 因此  $c_1 = c_{B_1} = \sum_{x \in G} x$ . 于是对于任意  $x \in G$  有  $xc_1 = c_1x = c_1$ . 所以  $xe_1 = e_1x = e_1$ . 因此又对于任意  $f \in A(G)$  有  $fe_1 = e_1f$ . 所以  $A(G)e_1$  中任意元能够表为  $fe_1 = f e_1 \cdot e_1 = e_1 f e_1 = \mu e_1 (\mu \in C)$  (由命题 34). 因此假如自这台得到的既約表現是  $\rho_1$ , 因为对于任意  $a \in G$ , 任意  $ue_1 \in A(G)e_1$  有  $\rho_1(a)(ue_1) = \mu a e_1 = ue_1$ , 所以  $\rho_1$  是恒等表現。

其次, 对于属于  $D^{(2)}$  的盘  $B_2$ ,  $\mathfrak{S}(B_2) = \{e\}$ ,  $\mathfrak{N}(B_2) = G$ . 于是  $c_2 = c_{B_2} = \sum_{x \in G} (\text{sgn } x)x$ . 因此与上同样, 对于任意  $x \in G$  有  $xe_2 = e_2x = (\text{sgn } x)e_2$ , 于是任意  $f e_2 \in A(G)e_2$  能够表为  $\mu' e_2 (\mu' \in C)$ . 所以假如自  $D^{(2)}$  得到的既約表現是  $\rho_2$ , 因为对于任意  $a \in G$ , 任意  $\mu' e_2 \in A(G)e_2$ ,

$$\rho_2(a)(\mu' e_2) = \mu' a e_2 = (\text{sgn } a) \mu' e_2,$$

所以  $\rho_2$  是交代表現。

例 5  $\mathfrak{S}_3$  的既約表現。

[解] 3 次的台是例 1 的三个。其中自第一及第三台分別得到恒等表現, 交代表現。为了求自第二台得到的既約表現, 取例 2 的盘 (左图), 这里

1	2
3	

$$c = 1 + (1, 2) - (1, 3) - (1, 3, 2),$$

由计算,  $c^2 = 3c$ . 所以这表现  $\rho$  是  $\frac{3!}{3} = 2$  次的表现. 因为作为  $A(G)c$  的基底, 可以取线性无关的任意两元, 乃取  $c$  与

$$f = (1\ 3)c = -1 + (1, 3) - (2, 3) + (1\ 2\ 3).$$

由这基底,  $\rho$  能够用下面的矩阵表现。

$$\begin{aligned} c &\leftrightarrow \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad (1, 2) \leftrightarrow \begin{pmatrix} 1 & -1 \\ 0 & -1 \end{pmatrix}, \quad (1, 3) \leftrightarrow \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \\ (2, 3) &\leftrightarrow \begin{pmatrix} -1 & 0 \\ -1 & 1 \end{pmatrix}, \quad (1\ 2\ 3) \leftrightarrow \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}, \quad (1\ 3\ 2) \leftrightarrow \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}. \end{aligned}$$

**注意** 这表现  $\rho$  的确是和在 177 頁中給出的表现  $\rho_2$  等价. 这事实能够直接予以证明, 即把  $\rho_2$  用矩阵

$$\begin{pmatrix} 0 & \frac{2}{\sqrt{3}} \\ -1 & \frac{1}{\sqrt{3}} \end{pmatrix}$$

变换就可以得到上面的  $\rho$ .

## § 39 标准盘

由前节定理 30, 求  $G = \mathfrak{S}_n$  的既约表现, 首先作記載  $n$  个数字的台  $D_1, \dots, D_q$ , 任取属于各个台的盘  $B_i, i = 1, \dots, q$ , 作各  $B_i$  的 Young 的对称子  $c_{B_i}, i = 1, \dots, q$ . 这样, 因为  $A(G)c_{B_i}$  是既约表现的表现空间, 所以由计算也能够作出既约表现的矩阵. 于是求对称群的既约表现的问题在理論上是解决了的, 但我们希望把自  $c_{B_i}$  得到的表现稍为具体的写出. 另外这表现的级数  $d_i$  由  $D_i$  的形状立即知道. 在下面两节介绍 Young 对于这问题的方法。

Young 为了这, 对于各个台象下面那样定义标准盘 (standard tableau), 它是满足条件

$$\begin{cases} i < i' \Rightarrow B(i, k) < B(i', k), \\ k < k' \Rightarrow B(i, k) < B(i, k') \end{cases}$$

的盘。



**例 1**  $n=3$  时, 对于台  $\begin{array}{|c|c|}\hline & \\ \hline & \\ \hline\end{array}$  有  $\begin{array}{|c|c|}\hline 1 & 2 \\ \hline 3 & \\ \hline\end{array}$ ,  $\begin{array}{|c|c|}\hline 1 & 3 \\ \hline 2 & \\ \hline\end{array}$  两个标准盘。  $n=5$  时, 对于台  $\begin{array}{|c|c|}\hline & \\ \hline & \\ \hline\end{array}$  的标准盘有下面五个:

$$\begin{array}{|c|c|}\hline 1 & 2 \\ \hline 4 & 5 \\ \hline\end{array} \begin{array}{|c|c|}\hline 1 & 2 \\ \hline 3 & 5 \\ \hline\end{array} \begin{array}{|c|c|}\hline 1 & 2 \\ \hline 3 & 4 \\ \hline\end{array} \begin{array}{|c|c|}\hline 1 & 3 \\ \hline 2 & 5 \\ \hline\end{array} \begin{array}{|c|c|}\hline 1 & 3 \\ \hline 2 & 4 \\ \hline\end{array}$$

对于各个台  $D$ , 能有几个标准盘? 但是对于  $D$  所能作的标准盘的总数象在下节所示, 是等于自  $c_B (B \in \mathfrak{B}(D))$  所得到的既約表現的級数  $d_i$ 。

以下假定对应于  $n$  的分割

$$n = m_1 + m_2 + \cdots + m_r, \quad m_1 \geq m_2 \geq \cdots \geq m_r > 0$$

的台用  $D(m_1, \cdots, m_r)$  表示。  $D(m_1, \cdots, m_r)$  持有  $r$  行, 在第  $i$  行附着  $m_i$  个数字。对于台  $D(m_1, \cdots, m_r)$  形成的标准盘的总数用  $d(m_1, \cdots, m_r)$  表示。关于这有下面的命题。

#### 命题 41

$$\sum_{\substack{m_1 + \cdots + m_r = n \\ m_1 \geq \cdots \geq m_r > 0 \\ r=1, 2, \cdots, n}} (d(m_1, \cdots, m_r))^2 = n! \quad (39.1)$$

为証此, 需要几个引理。首先引入下面的記法。

把  $n = \sum_{i=1}^r m_i$  次台  $D(m_1, \cdots, m_r)$  暂时固定, 它用  $D$  表示, 又把  $d(m_1, \cdots, m_r)$  略記为  $d$ 。假定  $m_{s-1} > m_s$ , 那末在  $D$  的第  $s$  行的右端又添加一个格子就得到  $(n+1)$  次台  $D(m_1, \cdots, m_{s-1}, m_s+1, m_{s+1}, \cdots, m_r)$ 。这台用  $D^{(s)}$  表示,  $D^{(s)}$  上标准盘的个数用  $d^{(s)}$  表示。假如  $m_{s-1} = m_s$ , 那末  $D^{(s)}$  不存在。这时命  $d^{(s)} = 0$ 。又假定  $D^{(r+1)} = D(m_1, \cdots, m_r, 1)$ , 它上标准盘的个数作为  $d^{(r+1)}$ 。又在同一个  $D$ , 假如  $m_t > m_{t+1}$ , 那末除去  $D$  的第  $t$  行右端一个格子就得到  $(n-1)$  次台  $D(m_1, \cdots, m_{t-1}, m_t-1, m_{t+1}, \cdots, m_r)$ , 这台用  $D_{(t)}$  表示。  $D_{(t)}$  上标准盘的个数假定是  $d_{(t)}$ 。假如  $m_t = m_{t+1}$ , 那

末  $D_{(t)}$  不存在。这时命  $d_{(t)} = 0$ 。再又假如  $m_r > 1$ , 那末  $D_{(r)} = D(m_1, \dots, m_{r-1}, m_r - 1)$ , 假如  $m_r = 1$ , 那末  $D_{(r)} = (m_1, \dots, m_{r-1})$ . 当  $m_{p-1} > m_p > m_{p+1}$  时, 显然  $(d_{(p)})^{(p)} = (d^{(p)})_{(p)} = d$ . 特别,  $(d_{(r)})^{(r)} = (d^{(r-1)})_{(r+1)} = d$ . 一般, 假定  $d^{(s)} \neq 0$ ,  $d_{(t)} \neq 0$ , 那末  $(d^{(s)})_{(t)} = (d_{(t)})^{(s)}$ , 因此把它单写成  $d_{(t)}^{(s)}$ . 当  $d^{(s)} = 0$  或  $d_{(t)} = 0$  时,  $d_{(t)}^{(s)} = 0$ .

**引理 1** 在台  $D = D(m_1, \dots, m_r)$  上任意标准盘  $B$  中, 数字  $n$  必在某行的右端, 如果  $n$  所在的行是第  $t$  行, 那末  $m_t > m_{t+1}$ .

**证明** 由标准盘的定义显然。

**引理 2**  $n$  在第  $t$  行的标准盘的个数等于  $d_{(t)}$ .

**证明**  $n$  在第  $t$  行的标准盘存在时, 由引理 1,  $n$  在第  $t$  行的右端, 而  $m_t > m_{t+1}$ . 于是假如把这标准盘中数字  $n$  所在的格子除去就得到  $D_t$  上的标准盘。反之, 对于  $D_t$  上一个标准盘, 在第  $t$  行的右端添加一个格子, 如果在这里记为  $n$ , 就得到  $n$  在第  $t$  行的  $D$  的标准盘。于是这时引理 2 成立。在这以外的情况, 即  $m_t = m_{t+1}$  时,  $n$  在第  $t$  行的标准盘不存在, 由定义,  $d_{(t)} = 0$ . 所以这时引理 2 也成立。

**引理 3**

$$d = \sum_{t=1}^r d_{(t)}. \quad (39.2)$$

**证明** 由引理 2 显然成立。

**例 2** 用引理 3, 能够计算对于任意台的标准盘的个数。例如如果就例 1 中两个台来计算,

$$d(2, 1) = d(1, 1) + d(2) = d(1) + d(1) = 1 + 1 = 2,$$

$$\begin{aligned} d(3, 2) &= d(2, 2) + d(3, 1) = 2d(2, 1) + d(3) \\ &= 2d(2, 1) + d(1) = 2 \times 2 + 1 = 5. \end{aligned}$$

**引理 4**

$$(n+1)d = \sum_{s=1}^{r+1} d^{(s)}. \quad (39.3)$$

**証明** 假定  $n=1$ , 那末

$$D = \square, \quad D^{(1)} = \begin{bmatrix} \square & \square \end{bmatrix}, \quad D^{(2)} = \begin{bmatrix} \square \\ \square \end{bmatrix}.$$

因此  $d = d^{(1)} - d^{(2)} = 1$ , 所以 (39.3) 成立。于是由归纳法, 假定关于  $(n-1)$  次台 (39.3) 成立, 来证明关于  $n$  次台的 (39.3)。

由归纳法的假定,

$$nd_{(t)} = \sum_{s=1}^{r+1} d_{(t)}^{(s)} \quad (1)$$

关于  $t=1, \dots, r$  成立。又关于  $D^{(s)}$ ,  $s=1, \dots, r$ , 如果用引理 3, 那末

$$d^{(s)} = \sum_{t=1}^r d_{(t)}^{(s)}. \quad (2)$$

因为关于  $D^{(r+1)}$  行数是  $r+1$ , 所以

$$d^{(r+1)} = \sum_{t=1}^r d_{(t)}^{(r+1)} + (d^{(r+1)})_{(r+1)} = \sum_{t=1}^r d_{(t)}^{(r+1)} + d. \quad (3)$$

用 (1), (2), (3) 计算 (39.3) 的右边得

$$\begin{aligned} \sum_{s=1}^{r+1} d^{(s)} &= \sum_{s=1}^r \sum_{t=1}^r d_{(t)}^{(s)} + \sum_{t=1}^r d_{(t)}^{(r+1)} + d = \sum_{t=1}^r \sum_{s=1}^{r+1} d_{(t)}^{(s)} + d \\ &= n \sum_{t=1}^r d_{(t)} + d = (n+1)d. \end{aligned}$$

**命题 41 的证明** 关于  $n$  用归纳法来证明。因为  $n=1$  时是显然的, 所以关于  $n$  假定命题成立来证明关于  $n+1$  即可。

对于  $n$  次台附加一列番号, 假定为  $D_1, \dots, D_q$ ,  $D_i$  上标准盘的个数作为  $d_i$ , 于是 (39.1) 能够用

$$\sum_{i=1}^q d_i^2 = n! \quad (4)$$

表示。假定  $(n+1)$  次台是  $\bar{D}_1, \dots, \bar{D}_q$ ,  $\bar{D}_j$  上标准盘的个数是  $\bar{d}_j$ , 今假定 (4) 成立, 证明

$$\sum_{j=1}^q \bar{d}_j^2 = (n+1)! \quad (5)$$

即可。在  $D_i$  中一行的右端添加一个格子成为  $\bar{D}_j$  时,  $D_i, \bar{D}_j$  相差只有一个格子。假定用記号  $i \sim j$  表示。于是作  $i \sim j$  这样的  $i, j$  組  $(i, j)$  的全体的积  $d_i \bar{d}_j$ , 假如它們的和是  $s$ ,

$$s = \sum_{i \sim j} d_i \bar{d}_j,$$

这  $s$  的意义能够从两方面来考虑。首先, 假如把  $i$  固定, 作关于  $i \sim j$  这样  $j$  的  $d_i \bar{d}_j$  的和  $s_i$ , 于是

$$s = s_1 + \cdots + s_q. \quad (6)$$

再假定先把  $j$  固定, 作关于  $i \sim j$  这样  $i$  的  $d_i \bar{d}_j$  的和  $\bar{s}_j$ , 于是

$$s = \bar{s}_1 + \cdots + \bar{s}_q. \quad (7)$$

如果象 (6) 那样考虑, 用 (39.3), 因为

$$s_i = d_i \sum_{i \sim j} \bar{d}_j = (n+1) d_i^2,$$

所以由 (4),  $s = (n+1) 1 = (5)$  的右边。如果象 (7) 那样来考虑, 用 (39.2),

$$\bar{s}_j = \bar{d}_j \sum_{i \sim j} d_i = \bar{d}_j^2,$$

所以  $s = (5)$  的左边。因此 (5) 得証。

## § 40 标准盘的个数与对称群的既約表現的級数

在本节証明下面的定理。

**定理 31** 在  $n$  阶对称群  $\mathfrak{S}_n$  中, 自对应于台  $D$  上任意盘  $B$  的 Young 的对称子  $c_B$  所得到的表現  $\rho_B$  的級数等于  $D$  上标准盘的个数  $d_D$ 。

在前节已示明

$$\sum_D d_D^2 = n!. \quad (40.1)$$

引用这事实, 上定理 31 的証明归結于下面的命題。

**命題 42** 假定自台  $D$  上盘  $B_1, \cdots, B_n$  所得到的 Young 的对称子是  $c_1, \cdots, c_n$ , 那末  $A_D = A(G)c_1 + \cdots + A(G)c_n$  是  $A(G)$  的

最小兩側理想。特別，假如  $B_1, \dots, B_d$  是標準盤，那末

$$A(G)c_1 + \dots + A(G)c_d = A(G)c_1 \oplus \dots \oplus A(G)c_d.$$

實際上，這命題假如已證明，由定理 29， $A_D$  與任一個  $A^{(i)}$  一致，因此成為  $d_i$  個  $d_i$  級既約左理想的直和。這  $d_i$  不外是  $\rho_B$  的級數。一方面因為  $A(G)c_1 \oplus \dots \oplus A(G)c_d \subset A_D$  是  $d$  個既約左理想的直和，所以由定理 6'， $d_D \leq d_i$ 。這對各台（因而各  $i$ ）都成立。在  $q$  個  $d_i$  之間，由定理 17 系 1 有關係

$$\sum_{i=1}^q d_i^2 = n!.$$

由這及 (40.1)，不得不  $d_D = d_i$ 。

於是又更得下系。

**系**  $A_D, c_1, \dots, c_d$  假定如命題 42，那末

$$A_D = A(G)c_1 \oplus \dots \oplus A(G)c_d.$$

為了證明這命題，把  $D$  上標準盤排成辭書式的順序，假定為  $B_1 < B_2 < \dots < B_d$ 。

所謂辭書式是下面的意義。假定  $B, B'$  是  $D$  上兩個盤，比較依順序排列了的  $n$  個數字的列

$$B(1, 1), B(1, 2), \dots, B(1, m_1), B(2, 1), \dots, B(r, m_r),$$

$$B'(1, 1), B'(1, 2), \dots, B'(1, m_1), B'(2, 1), \dots, B'(r, m_r).$$

假如  $B \neq B'$ ，那末在其中有  $B(i, k) \neq B'(i, k)$  的  $(i, k)$  出現。依上順序看時對於最初出現相異的數字  $B(i, k), B'(i, k)$ ，如果  $B(i, k) < B'(i, k)$ ，那末  $B < B'$ 。

**例** 在台  $D = D(3, 2)$  上的標準盤

$$\begin{array}{|c|c|c|} \hline 1 & 2 & 3 \\ \hline 4 & 5 & \\ \hline \end{array} < \begin{array}{|c|c|c|} \hline 1 & 2 & 4 \\ \hline 3 & 5 & \\ \hline \end{array} < \begin{array}{|c|c|c|} \hline 1 & 2 & 5 \\ \hline 3 & 4 & \\ \hline \end{array}$$

$$< \begin{array}{|c|c|c|} \hline 1 & 3 & 4 \\ \hline 2 & 5 & \\ \hline \end{array} < \begin{array}{|c|c|c|} \hline 1 & 3 & 5 \\ \hline 2 & 4 & \\ \hline \end{array}$$

這時下面的引理成立。

**引理** 假定在  $D$  上两个标准盘  $B, B', B \gg B'$ , 那末  $B > B'$ .

**証明** 假定  $B < B'$ , 示明  $B \not> B'$  即可。对于  $(i, k)$  排成上面那样顺序, 取满足  $B(i, k) < B'(i, k)$  的最初  $(i, k)$ . 在这格子“上左”的格子中 (图中粗范围中的格子),  $B$  与  $B'$  的数字相同。这里  $i \neq 1$ , 即  $(i, k)$  不能在左端。在标准盘, 左端数字是由在它前的数字确定。又  $B(i, k)$  在  $B'$  中不能在  $(i, k)$  右下 (图中点线的范围)。因为  $B'(i, k)$  已经是比  $B(i, k)$

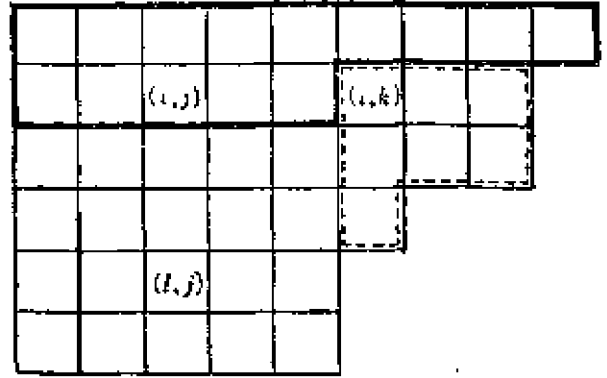


图 40.1

大, 所以如果  $B(i, k) = B'(l, j)$ , 那末  $i < l, j < k$ . 这时  $(i, j)$  的格子因为在  $(i, k)$  的“上左”, 所以  $B(i, j) = B'(i, j)$ . 于是  $B(i, j), B(i, k)$  这两数字在  $B$  中是在同行, 在  $B'$  中  $B'(i, j), B'(l, j)$  则在同列。

**系** 假如  $B < B'$ , 那末  $c_B c_{B'} = 0$ .

**証明** 由上面引理及命题 39 即得。

**命题 42 的証明**  $A_D$  显然是  $A(G)$  的左理想, 更来証明又是右理想。于是假定  $a \in G$ , 把  $a$  看成  $A(G)$  的基底中元  $f_a$  而来証明  $A_D a = A_D$  即可。由命题 28, 因为有为  $a^{-1} c_i a = c_{v_i}$  即  $c_i a = a c_{v_i}$ , 这样  $\{1, 2, \dots, n!\}$  的排列  $\{v_1, v_2, \dots, v_{n!}\}$ , 所以

$$(x_1 c_1 + \dots + x_{n!} c_{n!}) a = x_1 a c_{v_1} + \dots + x_{n!} a c_{v_{n!}} \in A_D.$$

因此  $A_D$  是两侧理想。

假定  $A_D$  是含  $c_1$  的两侧理想,  $A_0$  含  $c_1$  的最小两侧理想, 因为  $c_1, \dots, c_{n!}$  是相互等价的幂等元的数量倍, 所以由命题 23,  $c_2, \dots, c_{n!} \in A_0$ , 因此  $A_0 \supset A_D$ , 于是  $A_0 = A_D$ . 所以  $A_D$  是  $A(G)$  的最小两侧理想。

在証明后半部, 示明  $x_1 c_1 + \cdots + x_d c_d = 0 (x_i \in A(G)) \Rightarrow x_1 c_1 = \cdots = x_d c_d = 0$  即可。今假定标准盘  $B_1, \cdots, B_d$  取排成  $B_1 < \cdots < B_d$  順序的番号, 如果  $x_1 c_1 + \cdots + x_d c_d = 0$ , 那末自右乘  $c_1$  得  $x_1 c_1^2 = 0$ , 所以  $x_1 c_1 = 0$ . 因此  $x_2 c_2 + \cdots + x_d c_d = 0$ . 假如自右乘  $c_2$  就得到  $x_2 c_2 = 0$ . 以下同样即得  $x_1 c_1 = x_2 c_2 = \cdots = x_d c_d = 0$ .

注意 对于台  $D$  上标准盘的个数  $d_D$  (即对应于  $D$  上盘  $B$  的既約表現  $\rho_B$  的級数) 下面的明晰 (explicit) 公式是大家熟知的<sup>①</sup>:

$$d_D = n! \frac{\prod_{i < j} (l_i - l_j)}{l_1! l_2! \cdots l_r!}.$$

但  $D = D(m_1, m_2, \cdots, m_r)$ ,  $l_i = m_i + r - i$ .

当  $n$  不太大时, 实际計算  $d_D$  用前节例 2 所用的前节引理 3 的方法比用这公式还要便利。

最后, 把  $\rho_B$  的特征标明显 (explicit) 給出的 (Schur) 公式和計算这特征标相当于前节引理 3 的 (Murnaghan) 方法也是大家熟知的, 关于这方面的介紹于此皆从略。

### § 41 对称群的既約表現的矩陣

本节根据 Young 叙述实际計算对称群既約表現矩陣的方法。

与前节同样, 假定把  $D$  上标准盘辞书式地排列为  $B_1 < B_2 < \cdots < B_d$ ,  $c_i$  是  $B_i$  的对称子 (以下  $D$  认为是一定的, “ $D$  上” 这語不再一一声明)。又关于两个盘  $B, B'$ , § 38 中的記法  $\mathfrak{S}_B, \mathfrak{S}_{B'}$  分别写成  $\mathfrak{S}, \mathfrak{S}'$ , 它們的元分别写成  $h, h'$ , 把  $H_B, H_{B'}$  分别写成  $H, H'$ , 关于  $\mathfrak{S}, K, k$  也用同样的記法 ( $B_i, B_j$  代替  $B, B'$  时, 与它对应的写成  $H_i, H_j, K_i, K_j$  等)。再关于两个番号  $i, j (1 \leq i, j \leq d)$ , 把  $B_i > B_j$  写成  $i > j$ , 把  $B_i \gg B_j$  写成  $i \gg j$ . 由前节引理, 假如  $i > j$ , 那末  $i \geq j$ . 假如  $i \gg j$ , 那末  $i > j$ . 又由命题 39, 假如  $i \succ j$ , 那末

① 参看 F. D. Murnaghan: The Theory of Groups Representations (1938) p. 114~119. — 譯者注

$$H_i K_j = K_j H_i = 0, \quad e_i c_i = 0.$$

**命题 43** 假定关于两个盘  $B, B'$  有  $B \succ B'$ , 那末  $\mathfrak{S}$  中存在满足  $K'h = -hK$  的元  $h$ .

**证明** 因为  $B \succ B'$ , 所以由命题 30, 由  $xB = B'$  确定的  $x \in G$  能够写成  $x = hk$ ,  $h \in \mathfrak{S}$ ,  $k \in \mathfrak{R}$  的形状。由命题 28,

$$K' = xKx^{-1} = hkKk^{-1}h^{-1} = hKh^{-1}.$$

所以  $K'h = hK$ . (证毕)

以下考虑有顺序的标准盘  $B_1 < \cdots < B_d$ . 对于  $i \in \{1, 2, \dots, d\} = J$ , 假如取成为  $i \ll j$  的  $j \in J$ , 当然  $i < j$ . 并且由命题 43, 存在  $K'h_j = h_j K_i$  这样的  $h_j \in \mathfrak{S}_j$ . 这  $h_j$  用  $h_{ij}$  表示。在命题 43 的证明中, 给出求  $h_{ij}$  的方法。即取满足  $a_{ij}B_j = B_i$  这样的  $a_{ij} \in G$ , 由  $a_{ij} = h_{ij}k_{ij}$ ,  $h_{ij} \in \mathfrak{S}_j$ ,  $k_{ij} \in \mathfrak{R}_j$  给出。由命题 27,  $h_{ij}$  由  $i$  与  $j$  ( $i \ll j$ ) 唯一地给出。当  $i = j$  或  $i \not\ll j$  时,  $h_{ij} = 0 (\in A(G))$ . 用这  $h_{ij}$  由

$$u_d = e,$$

$$u_{d-1} = e - h_{d-1, d},$$

$$u_{d-2} = e - h_{d-2, d-1}u_{d-1} - h_{d-2, d},$$

$$\dots\dots\dots,$$

$$u_1 = e - h_{1, 2}u_2 - h_{1, 3}u_3 - \cdots - h_{1, d-1}u_{d-1} - h_{1, d}u_d$$

( $e$  是  $G$  的单位元) 顺次定义  $u_d, u_{d-1}, \dots, u_1 \in A(G)$ , 命

$$K'_i = K_i u_i \quad (i = 1, \dots, d).$$

关于这  $K'_i$ , 下面的命题成立。

**命题 44** (1)  $K'_i = K_i = \sum_{j=1}^d h_{ij} K'_j$ .

(2) 假如  $i \neq j$ , 那末  $K'_i H_j = 0$ ,  $i, j = 1, \dots, d$ .

(3)  $K'_i H_i = K_i H_i$ .

**证明** (1) 由  $K'_i, h_{ij}$  的定义自明。

(2), (3) 用关于  $i$  自上而下的归纳法来证明。假定  $i = d$ , 那末  $K'_d = K_d$ . 所以 (3) 显然成立。又因为  $B_i < B_d$ , 由命题 39, (2)



也是显然的。于是对于  $i < p \leq d$  的所有自然数  $p$ , 假定

$$\begin{cases} K'_p H_j = 0, & j = 1, \dots, d, j \neq p, \\ K'_i H_p = K_p H_p \end{cases}$$

成立, 来证明 (2), (3)。

$$\text{由 (1), } K'_i H_j = K_i H_j - \sum_{p=1}^d h_{ip} K'_p H_j.$$

这里把关于  $j$  的情况分为下面三种:

(i) 假如  $i \prec j$ , 由命题 39,  $K_i H_j = 0$ . 对于  $p = i$  或  $p \succ i$  的  $p$  由定义,  $h_{ip} = 0$ . 对于  $p \gg i$  的  $p$ , 因为  $i < p \leq d$ ,  $p \neq j$ , 所以由归纳法的假定,  $K'_p H_j = 0$ . 因此  $K'_i H_j = 0$ .

(ii) 假如  $i \ll j$ , 那末对于  $p \gg i$ ,  $p \neq j$  的  $p$  与上同样,  $K'_i H_j = 0$ . 对于  $p = i$  或  $p \succ i$  的  $p$ , 因为  $h_{ip} = 0$ , 所以

$$K'_i H_j = K_i H_j - h_{ij} K'_j H_i.$$

于是用归纳法假定的第二式, 得

$$\begin{aligned} K'_i H_j &= K_i H_j - h_{ij} K'_j H_i = K_i H_j - K_i h_{ij} H_i \\ &= K_i H_j - K_i H_j = 0. \end{aligned}$$

由 (i) 与 (ii), 得证 (2)。

(iii)  $i = j$  时, 用 (2),  $K'_i H_i = K_i H_i - h_{ii} K'_i H_i = K_i H_i$ . 因此 (3) 得证。

**命题 45** 假定  $c'_j = H_j K'_j = c_j u_j$ , 与命题 34 系, 命题 35 同样, 命  $\alpha = \frac{n!}{d}$ , 那末  $c'_j c_j = \alpha c_j \neq 0$ ,  $c'_j c'_j = \alpha c'_j$ . 又如果  $i \neq j$ , 那末  $c'_i c'_j = 0$ .

**证明**  $c'_j c_j = H_j K'_j H_j K_j$ . 由前命题 (3), 因为  $K'_j H_j = K_j H_j$ , 所以  $c'_j c_j = c_j c_j = \alpha c_j \neq 0$ ,  $c'_j c'_j = c'_j c_j u_j = \alpha c_j u_j = \alpha c'_j$ . 又

$$c'_i c'_j = H_i K'_i H_j K'_j = 0 \quad (i \neq j).$$

系  $\frac{1}{\alpha} c'_j$  是  $A(G)$  中与  $\frac{1}{\alpha} c_j$  等价的既约幂等元。

**命题 46** 假定象 253 页那样,  $G$  中把  $B_j$  移动到  $B_i$  的元是

$a_{ij}(a_{ij}B_j - B_i)$ , 如果命  $\frac{1}{\alpha} a_{ij}c'_j = e_{ij}$ , 那末  $e_{ij}e_{kl} = \delta_{jk}e_{il}$ .

**証明** 由命題 28,  $a_{ij}H_j = H_i a_{ij}$ ,  $a_{ij}K_j = K_i a_{ij}$ , 所以

$$e_{ij}e_{kl} = \frac{1}{\alpha^2} a_{ij}H_j K'_j a_{kl}H_l K'_l = \frac{1}{\alpha^2} a_{ij}H_j K'_j H_k a_{kl} K'_l.$$

但由命題 44(2), 如果  $j \neq k$ , 那末  $K'_j H_k = 0$ . 因此, 假如  $j \neq k$ , 那末  $e_{ij}e_{kl} = 0$ . 又假如  $j = k$ , 那末  $K'_j H_k = K'_j H_j = K_j H_j$ . 因此用  $a_{ij}a_{kl} = a_{il}$  能够象下面这样来証明,

$$\begin{aligned} e_{ij}e_{kl} &= \frac{1}{\alpha^2} a_{ij}H_j K'_j H_j a_{kl} K'_l = \frac{1}{\alpha^2} a_{ij}a_{kl}H_i K_l H_l K'_l \\ &= \frac{1}{\alpha^2} a_{il}H_i K'_l H_l K'_l = \frac{1}{\alpha^2} a_{il}c'_l c'_l \\ &= \frac{1}{\alpha^2} a_{il} \alpha c'_l = \frac{1}{\alpha} a_{il}c'_l = e_{il}. \end{aligned}$$

**命題 47**  $e_{11}, e_{12}, \dots, e_{dd}$  是含  $c_i$  或  $c'_i$  的  $A(G)$  中最小兩側理想  $A(G)c_1 + \dots + A(G)c_d = A_D$  的基底,  $\sum_{i=1}^d e_{ii} = e_D$  是  $A_D$  的單位元.

**証明** 因为  $e_{ij} = \frac{1}{\alpha} a_{ij}c'_j \in A(G)c'_j = A(G)c_j u_j \subset A_D$ , 所以  $e_{ij}$  含于所有的  $A_D$ .  $\dim A_D = d^2$ , 但  $d^2$  个元  $e_{11}, e_{12}, \dots, e_{dd}$  的綫性无关性可如下証明. 实际上, 假如  $\sum_{i,j=1}^d \alpha_{ij}e_{ij} = 0$ ,  $\alpha_{ij} \in \mathbb{C}$ , 于两边左乘  $e_{ii}$ , 右乘  $e_{jj}$  得  $\alpha_{ij}e_{ij} = 0$ . 因为  $e_{ij}e_{ji} = e_{ii} = \frac{1}{\alpha} c'_i \neq 0$ , 所以  $e_{ij} \neq 0$ . 于是  $\alpha_{ij} = 0$ . 因此  $e_{ij}$  是  $A_D$  的基底,  $A_D$  中任意元能够唯一地表为  $\sum_{i,j=1}^d \alpha_{ij}e_{ij}$  的形状. 假如对于这元使  $\mathfrak{M}(d, \mathbb{C})$  中元  $(\alpha_{ij})$  对应的映射是  $\varphi$ , 那末由前命題立即得知这样的  $\varphi$  是自  $A_D$  到  $\mathfrak{M}(d, \mathbb{C})$  作为代数的同构映射. 显然因为  $\varphi(e_D) = E_d$ , 所以  $e_D$  是  $A_D$  的單位元. (証毕)

用上命題中的同构映射  $\varphi$ , 能够象下面那样作成  $G$  的  $d$  級矩陣表現. 即如果把  $a \in G$  看成为  $A(G)$  中元, 那末  $ae_D \in A_D$ , 因为

$\varphi(ae_D) \in \mathfrak{M}(d, \mathbf{C})$ ,  $\varphi(abe_D) = \varphi(ae_D be_D) = \varphi(ae_D) \varphi(be_D)$ , 所以  $a \rightarrow \varphi(ae_D)$  給出  $G$  的表现。假定  $\varphi(ae_D) = (\alpha_{ij})$ , 与 § 37 例 4 同样, 把只是第  $i$  行第  $j$  列是 1, 其他元都是 0 的矩阵用  $E_{ij}$  表示, 因为  $\varphi(e_{ij}) = E_{ij}$ ,  $E_{ii} \cdot (\alpha_{ij}) \cdot E_{jj} = \alpha_{ij} E_{ij}$ , 所以

$$e_{ii} a e_{jj} = \alpha_{ij} e_{ij}. \quad (41.1)$$

如果把  $e_{ij}$  的定义  $e_{ij} = \frac{1}{\alpha} a_{ij} c'_j$  代入 (41.1), 那末 (用  $a_{ii} = e$ )

$$\frac{1}{\alpha} c'_i a c'_j = \alpha_{ij} a_{ij} c'_j. \quad (41.2)$$

把这左边变形与右边比較能够求出  $\alpha_{ij}$ . 为了簡明地叙述这求法, 引入下面的术语。

象前面那样, 对于  $i \in \{1, 2, \dots, d\} = J$ , 滿足  $i \ll i', i' \ll i'', \dots$  这样条件的  $\{i, i+1, \dots, d\}$  的子数列  $\{i, i', i'', \dots\}$  叫做  $i$  容許数列。  $i$  容許数列当然由  $(d-i+1)$  个以下的数构成,  $i$  容許数列的个数是有限的。这个数用  $s_i$  表示。对于  $i$  容許数列中各个数作  $G$  中元  $h_w h_{w'} \dots$ , 它叫做对应这容許数列的元。 ( $h_w$  等由前面的定义及命題 43 的証明, 由  $a_w B_i = B_i$ ,  $a_w = h_w \cdot k_w$ ,  $h_w \in \mathfrak{S}_i$ ,  $k_w \in \mathfrak{S}_i$  等給出)。在对应这等  $i$  容許数列的元中, 附以番号, 假定为  $r_i^{(1)}, \dots, r_i^{(s_i)}, \dots, r_i^{(s_i)}$ . 又把  $r_i^{(p)}$  作“因数”的数 (= (第  $p$  个  $i$  容許数列的长) - 1) 根据是偶数或奇数命  $\varepsilon_i^{(p)} = 1$  或  $-1$ . 又假定  $\varepsilon_i^{(0)} = 1$ ,  $r_i^{(0)} = e$ .

**引理** 对于 253 頁定义的  $u_i$ , 下面的公式成立:

$$u_i = \sum_{p=0}^{s_i} \varepsilon_i^{(p)} r_i^{(p)}. \quad (41.3)$$

**証明** 假如  $i=d$ , 那末 (41.3) 两边都是 1. 假如  $i=d-1$ , 由定义, 那末两边都是  $e - h_{i-1, d}$ . 一般关于  $d-i$  由归纳法容易推得。 (証毕)

为了把 (41.2) 的左边变形, 命  $(r_i^{(p)} a)^{-1} B_i = B_i^{(p)}$ ,  $c_{B_i^{(p)}} = c_i^{(p)}$ ,

于是由命题 28, 因为  $c_i r_i^{(\nu)} a = r_i^{(\nu)} a c_i^{(\nu)}$ , 所以

$$\begin{aligned} c'_i a c'_j &= c_i a_i a c'_j = c_i \left( \sum_{\nu=0}^{a_i} \varepsilon_i^{(\nu)} r_i^{(\nu)} \right) a c'_j = \sum_{\nu=0}^{a_i} \varepsilon_i^{(\nu)} c_i r_i^{(\nu)} a c'_j \\ &= \sum_{\nu=0}^{a_i} \varepsilon_i^{(\nu)} r_i^{(\nu)} a c_i^{(\nu)} c'_j. \end{aligned} \quad (41.4)$$

在这右边的項假如  $B_j \not\vdash B_i^{(\nu)}$ , 那末  $c_i^{(\nu)} c'_j = c_i^{(\nu)} c_j a_j = 0$ . 又假如  $B_j \gg B_i^{(\nu)}$ , 如果命  $a_{ij}^{(\nu)} B_j = B_i^{(\nu)}$ ,  $a_{ij}^{(\nu)} = h_{ij}^{(\nu)} k_{ij}^{(\nu)}$ ,  $h_{ij}^{(\nu)} \in \mathfrak{S}_j$ ,  $k_{ij}^{(\nu)} \in \mathfrak{S}_j$ , 那末

$$r_i^{(\nu)} a c_i^{(\nu)} c'_j = r_i^{(\nu)} a c_i^{(\nu)} c_j a_j = r_i^{(\nu)} a a_{ij}^{(\nu)} c_j (a_j^{(\nu)})^{-1} c_j a_j,$$

但

$$c_j (a_j^{(\nu)})^{-1} c_j = c_j (h_{ij}^{(\nu)} k_{ij}^{(\nu)})^{-1} c_j = (\operatorname{sgn} k_{ij}^{(\nu)}) c_j^2 = \alpha (\operatorname{sgn} k_{ij}^{(\nu)}) c_j.$$

又因为  $r_i^{(\nu)} a a_{ij}^{(\nu)} B_j = r_i^{(\nu)} a B_i^{(\nu)} = B_i$ ,

所以能够命  $r_i^{(\nu)} a a_{ij}^{(\nu)} = a_{ij}$ , 于是

$$r_i^{(\nu)} a c_i^{(\nu)} c'_j = \alpha (\operatorname{sgn} k_{ij}^{(\nu)}) a_{ij} c_j a_j = \alpha (\operatorname{sgn} k_{ij}^{(\nu)}) a_{ij} c'_j.$$

再假如  $B_j = B_i^{(\nu)}$ , 因为  $r_i^{(\nu)} a B_j = B_i$ , 所以

$$r_i^{(\nu)} a = a_{ij}, \quad c_i^{(\nu)} c'_j = c_j c'_j = a c'_j,$$

因此

$$r_i^{(\nu)} a c_i^{(\nu)} c'_j = \alpha a_{ij} c'_j.$$

于是假如  $B_j \not\vdash B_i^{(\nu)}$ , 那末  $\varepsilon_{ij}^{(\nu)} = 0$ , 假如  $B_j = B_i^{(\nu)}$ , 那末  $\varepsilon_{ij}^{(\nu)} = 1$ , 假如  $B_j \gg B_i^{(\nu)}$ , 如果命  $\varepsilon_{ij}^{(\nu)} = \operatorname{sgn} k_{ij}^{(\nu)}$ , 由 (41.4) 得

$$\frac{1}{\alpha} c'_i a c'_j = \left( \sum_{\nu=0}^{a_i} \varepsilon_i^{(\nu)} \varepsilon_{ij}^{(\nu)} \right) a_{ij} c'_j.$$

所以由 (41.2),

$$a_{ij} = \sum_{\nu=0}^{a_i} \varepsilon_i^{(\nu)} \varepsilon_{ij}^{(\nu)}. \quad (41.5)$$

这就是求  $a_{ij}$  的公式。总结以上得下定理。

**定理 32** 于  $n$  阶对称群  $\mathfrak{S}_n$ , 在属于对应于台  $D$  的既約表現  $\rho_D$  的一个矩陣表現中, 对应于  $a \in G$  的能够象下面那样求得。把  $D$  上标准盘辞书式的順序排列, 假定为  $B_1 < B_2 < \cdots < B_d$ ,  $d$  是  $\rho_D$  的級数。对于  $J = \{1, 2, \cdots, d\}$  中各元, 作  $i$  容許数列, 它的个数

假定是  $s_i (\geq 0)$ . 对应于各  $i$  容许数列的  $G$  中元假定是  $r_i^{(\nu)}$ ,  $\nu = 1, \dots, s_i$ . 命  $r_i^{(0)} = e$ . 又由第  $\nu$  个  $i$  容许数列的长是奇数, 是偶数因而命  $\varepsilon_i^{(\nu)} = +1$  或  $-1$ , 命  $\varepsilon_i^{(0)} = 1$ . 对于  $\nu = 0, 1, \dots, s_i$ , 命  $(r_i^{(\nu)} a)^{-1} B_i = B_i^{(\nu)}$ , 如果  $B_i^{(\nu)} \not\prec B_j$ , 那末  $\varepsilon_{ij}^{(\nu)} = 0$ , 如果  $B_i^{(\nu)} = B_j$ , 那末  $\varepsilon_{ij}^{(\nu)} = 1$ , 如果  $B_i^{(\nu)} \ll B_j$ , 那末命  $a_{ij}^{(\nu)} B_j = B_i^{(\nu)}$ ,  $a_{ij}^{(\nu)} = h_{ij}^{(\nu)} k_{ij}^{(\nu)}$ ,  $h_{ij}^{(\nu)} \in \mathfrak{S}_j$ ,  $k_{ij}^{(\nu)} \in \mathfrak{H}_j$ ,  $\text{sgn } k_{ij}^{(\nu)} = \varepsilon_{ij}^{(\nu)}$ . 这样定义  $\varepsilon_i^{(\nu)}$ ,  $\varepsilon_{ij}^{(\nu)}$  时, 由 (41.5) 给出的  $\alpha_{ij}$  的矩阵  $(\alpha_{ij})$  成为对应于  $a$  的  $\rho_D$  的表现矩阵.

**系**  $\mathfrak{S}_n$  的各既约表现类含有矩阵的所有元素都是有理整数的矩阵表现.

**证明** 因为在由定理 32 所作的表现矩阵中,  $\varepsilon_i^{(\nu)}$  所取的值是  $\pm 1$ ,  $\varepsilon_{ij}^{(\nu)}$  所取的值是 0 或  $\pm 1$ , 所以  $\alpha_{ij} \in \mathbb{Z}$ .

**例 1** 假定  $n = 3$ ,  $D = D(2, 1)$ , 那末

$$B_1 = \begin{bmatrix} 1 & 2 \\ 3 & \end{bmatrix}, \quad B_2 = \begin{bmatrix} 1 & 3 \\ 2 & \end{bmatrix}, \quad d=2.$$

这时因为  $1 \not\prec 2$ , 所以  $s_1 = 0$ .  $s_2$  当然是 0. 于是这时在 (41.5) 右边只有一项, 因为  $\varepsilon_i^{(0)} = 1$ ,  $r_i^{(0)} = e$ , 所以

$$\alpha_{ij} = \varepsilon_{ij}^{(0)}, \quad a^{-1} B_i = B_i^{(0)}.$$

今试求对于  $a = (1\ 2)$  的表现矩阵. 这时因为

$$B_1^{(0)} = (1\ 2) B_1 = \begin{bmatrix} 2 & 1 \\ 3 & \end{bmatrix}, \quad B_2^{(0)} = (1\ 2) B_2 = \begin{bmatrix} 2 & 3 \\ 1 & \end{bmatrix}$$

	$B_1$	$B_2$
$B_1^{(0)}$	1	-1
$B_2^{(0)}$	0	-1

$$\begin{aligned} B_1^{(0)} &\ll B_1 & (1\ 2) B_1 &= B_1^{(0)}, (1\ 2) \in \mathfrak{S}_1, e \in \mathfrak{H}_1, \\ B_1^{(0)} &\ll B_2 & (1\ 3) (1\ 2) B_2 &= B_1^{(0)}, (1\ 3) \in \mathfrak{S}_2, (1\ 2) \in \mathfrak{H}_2, \\ B_2^{(0)} &\not\prec B_1 \\ B_2^{(0)} &\ll B_2 & (1\ 2) B_2 &= B_2^{(0)}, & (1\ 2) \in \mathfrak{H}_2, \end{aligned}$$

所以  $\alpha_{ij} = \varepsilon_{ij}^{(0)}$  的值如左表.

于是  $(1\ 2) \rightarrow \begin{pmatrix} 1 & -1 \\ 0 & -1 \end{pmatrix}$ , 同样得  $(1\ 3) \rightarrow \begin{pmatrix} -1 & 0 \\ -1 & 1 \end{pmatrix}$ . 因为  $\mathfrak{S}_3$  能够用  $(1\ 2)$ ,

$(1\ 3)$  生成, 所以用矩阵乘法由它能够求得对应于  $\mathfrak{S}_3$  中各元的矩阵. (在这表

现中矩阵的元素都是 0 或  $\pm 1$ .)

例 2 假定  $n=5$ ,  $D=D(3, 2)$ , 由 § 40, 例 1 得

$$B_1 = \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & \end{bmatrix}, \quad B_2 = \begin{bmatrix} 1 & 2 & 4 \\ 3 & 5 & \end{bmatrix}, \quad B_3 = \begin{bmatrix} 1 & 2 & 5 \\ 3 & 4 & \end{bmatrix},$$

$$B_4 = \begin{bmatrix} 1 & 3 & 4 \\ 2 & 5 & \end{bmatrix}, \quad B_5 = \begin{bmatrix} 1 & 3 & 5 \\ 2 & 4 & \end{bmatrix}, \quad d_5 = 5.$$

这时因为  $1 \ll 5$ , 所以  $\{1, 5\}$  是 1 容许数列, 其他情况为  $i < j \Rightarrow i \ll j$  而对于  $i \geq 2$ ,  $i$  容许数列不存在, 1 容许数列也只有  $\{1, 5\}$ , 即  $s_1 = 1$ ,  $s_2 = s_3 = s_4 = s_5 = 0$ .  $a_{15} = (2\ 4\ 5\ 3) = (2\ 4)(3\ 5)(3\ 4) = (2\ 5)(2\ 4)(3\ 5)$ ,  $r_1^{(1)} = h_{15} = (2\ 4)(3\ 5)$ ,  $(k_{15} = (3\ 4))$ ,  $\varepsilon_1^{(1)} = -1$ . 于是试求对于  $\alpha = (1, 2)$  的表现矩阵.

$$\begin{cases} \alpha_{1j} = \varepsilon_{1j}^{(0)} - \varepsilon_{1j}^{(1)}, \\ \alpha_{ij} = \varepsilon_{ij}^{(0)}, \quad i \geq 2, \end{cases} \quad (1)$$

$$(r_1^{(0)}\alpha)^{-1}B_i = (1\ 2)B_i = B_i^{(0)},$$

因此

$$B_1^{(0)} = \begin{bmatrix} 2 & 1 & 3 \\ 4 & 5 & \end{bmatrix}, \quad B_2^{(0)} = \begin{bmatrix} 2 & 1 & 4 \\ 3 & 5 & \end{bmatrix},$$

$$B_3^{(0)} = \begin{bmatrix} 2 & 1 & 5 \\ 3 & 4 & \end{bmatrix}, \quad B_4^{(0)} = \begin{bmatrix} 2 & 3 & 4 \\ 1 & 5 & \end{bmatrix}, \quad B_5^{(0)} = \begin{bmatrix} 2 & 3 & 5 \\ 1 & 4 & \end{bmatrix}$$

又

$$(r_1^{(0)}\alpha)^{-1}B_i = (1\ 2)(3\ 5)(2\ 4)B_1 = \begin{bmatrix} 2 & 4 & 5 \\ 1 & 3 & \end{bmatrix} = B_1^{(1)}.$$

由这与前例同样自下表得到所求矩阵.

	$B_1$	$B_2$	$B_3$	$B_4$	$B_5$
$B_1^{(0)}, B_1^{(1)}$	1, 0	0, 0	0, 0	-1, 0	0, 1
$B_2^{(0)}$	0	1	0	-1	0
$B_3^{(0)}$	0	0	1	0	-1
$B_4^{(0)}$	0	0	0	-1	0
$B_5^{(0)}$	0	0	0	0	-1

例如,  $B_1^{(0)} \ll B_1$ ,  $(1\ 2)B_1 = B_1^{(0)}$ ,  $(1\ 2) \in \mathfrak{S}_1$ , 所以  $\varepsilon_{11}^{(0)} = 1$ . 因为  $B_1^{(1)} \not\subset B_1$ , 因此  $\varepsilon_{11}^{(1)} = 0$ . 于是把 1, 0 記入左上位置, 由 (1) 得

$$(1\ 2) \rightarrow \begin{pmatrix} 1 & 0 & 0 & -1 & -1 \\ 0 & 1 & 0 & -1 & 0 \\ 0 & 0 & 1 & 0 & -1 \\ 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & -1 \end{pmatrix}.$$

同样

$$(1\ 2\ 3\ 4\ 5) \rightarrow \begin{pmatrix} -1 & -1 & 1 & 1 & 0 \\ -1 & 0 & 0 & 0 & 1 \\ 0 & -1 & 0 & 0 & 0 \\ -1 & 0 & 0 & 1 & 0 \\ 0 & -1 & 0 & 1 & 0 \end{pmatrix}.$$

因为  $\mathfrak{S}_5$  能够用  $(1\ 2)$ ,  $(1\ 2\ 3\ 4\ 5)$  生成, 所以对应于其他元的矩陣都能够由上面两个相乘得出。

## § 42 Weyl 的相互律

在上 4 节 (§ 38~§ 41), 假定  $G = \mathfrak{S}_n$ , 但在这节  $G$  假定是一般的有限群, 把  $G$  的群代数  $A(G)$  略記为  $A$ . 又假定  $\rho$  是  $G$  的一个表現 (不是既約的也可),  $\rho$  的表現空間是  $V$ .

在 § 26, 把  $\mathfrak{L}(V)$  的任意子集合, 命名为  $\mathfrak{U}(V)$ . 对于  $\mathfrak{U}(V)$  集合  $S$ ,

$$\{\tau; \tau \in \mathfrak{L}(V), \forall \sigma \in S, \sigma\tau = \tau\sigma\}$$

形成的  $\mathfrak{U}(V)$  集合記成  $S'$ ,  $S'$  已証明是  $\mathbb{C}$  上代数。把  $S'$  也記成  $\mathfrak{C}(S)$ , 叫做  $S$  的**交換子代数**。 $\rho(G) = \{\rho(x); x \in G\}$  是一个  $\mathfrak{U}(V)$  集合, 今命  $\mathfrak{C}(\rho(G)) = Z$ . 因为  $Z$  中元当然是  $\mathfrak{L}(V)$  中元, 所以对于  $\zeta \in Z$ ,  $v \in V$  有  $\zeta(v) \in V$ .  $V$  的子空間  $W$ , 对于  $Z$  中任意元  $\zeta$  滿足  $\zeta(W) \subset W$  时,  $W$  叫做**对于  $Z$  不变** (或  **$Z$ -不变**)。

H. Weyl 在他的“群論与量子力学”(1928 初版) 中最后一章討論了量子力学中“对称問題”的对称群与旋轉群表現的关系, 在

再版(1931)中,他用代数方法証明了当  $G = \mathfrak{S}_n$  时  $A = A(G) = A(\mathfrak{S}_n)$  的左理想与对  $Z$  不变的  $V$  的子空間之間“相互律”(后面的定理 33) 成立,把初版的理論簡化。茲介紹如下。

首先假定  $V$  的对偶空間 (§ 10) 是  $\hat{V}$ 。对于  $u \in V$ ,  $\varphi \in \hat{V}$  把  $[u, \varphi] \in A$  用下式定义:

$$[u, \varphi](x) = \varphi(\rho(x)u) = (\rho(x)u, \varphi), \quad x \in G. \quad (42.1)$$

(第三边的內积是 § 10, 47 頁的意义)。于是下面的命題成立。

**命題 48**  $[u, \varphi]$  关于  $u, \varphi$  是双綫性的。即对于  $\lambda \in C$ ,  $u, v \in V, \varphi, \psi \in \hat{V}$ ,

$$[u+v, \varphi] = [u, \varphi] + [v, \varphi], \quad [\lambda u, \varphi] = \lambda[u, \varphi],$$

$$[u, \varphi + \psi] = [u, \varphi] + [u, \psi], \quad [u, \lambda\varphi] = \lambda[u, \varphi].$$

**証明** 由定义(42.1)自明。

**命題 49** 假如  $[u, \varphi] = [v, \varphi]$  关于所有的  $\varphi \in \hat{V}$  成立, 那末  $u = v$ 。

**証明** 因为由前命題,  $[u, \varphi] - [v, \varphi] = [u - v, \varphi]$ , 所以証明  $(\forall \varphi \in \hat{V}, [u, \varphi] = 0) \Rightarrow u = 0$  即可。但

$$\forall \varphi \in \hat{V}, [u, \varphi](e) = \varphi(\rho(e)u) = \varphi(u) = 0,$$

所以  $u = 0$ . (証毕)

其次, 象在 § 29 例 5 叙述那样, 把  $\rho$  的定义域自  $G$  根据  $\rho(\sum_{x \in G} \lambda_x f_x) = \sum_{x \in G} \lambda_x \rho(x)$  擴張到  $A$ . 自擴張了的  $A$  到  $GL(V)$  的映射仍記成  $\rho$ . 又对于  $f \in A$ , 用

$$\hat{f}(x) = f(x^{-1}), \quad x \in G$$

定义  $\hat{f} \in A$ .

**例 1**  $\widehat{fg} = \hat{g}\hat{f}, \hat{\hat{f}} = f$ .

[解] 由定义显然。

**例 2** 对于定义于 237 頁的  $H, K, c$ , 則  $\hat{H} = H, \hat{K} = K, \hat{c} = KI$  成立。

[解]  $H(x) = \begin{cases} 1 & (x \in \mathfrak{S}), \\ 0 & (x \notin \mathfrak{S}). \end{cases} \quad \hat{H}(x) = H(x^{-1}) = \begin{cases} 1 & (x^{-1} \in \mathfrak{S}), \\ 0 & (x^{-1} \notin \mathfrak{S}). \end{cases}$



因为  $\mathfrak{S}$  成群, 所以  $x \in \mathfrak{S} \Leftrightarrow x^{-1} \in \mathfrak{S}$ , 因此  $\widehat{H} = \widehat{H}$ , 同样  $\widehat{K} = \widehat{K}$ , 因而

$$\widehat{\hat{c}} = (\widehat{H\widehat{K}}) = \widehat{K}\widehat{H} = KH.$$

**命题 50** 对于  $f \in A$ , 有  $f[u, \varphi] = [u, {}^t(\rho(\hat{f}))\varphi]$ . ( ${}^t(\rho(\hat{f}))$  表示  $\rho(\hat{f})$  的轉置映射.)

**証明** 由 § 29 中  $A$  的积的定义,

$$\begin{aligned} (f[u, \varphi])(x) &= \sum_{y \in G} f(y^{-1})([u, \varphi](yx)) \\ &= \sum_{y \in G} f(y^{-1})(\rho(yx)u, \varphi) \\ &= \sum_{y \in G} f(y^{-1})(\rho(y)\rho(x)u, \varphi) \\ &= \left(\sum_{y \in G} f(y^{-1})\rho(y)\rho(x)u, \varphi\right) \\ &= (\rho(\hat{f})\rho(x)u, \varphi) \\ &= (\rho(x)u, {}^t(\rho(\hat{f}))\varphi). \end{aligned}$$

**命题 51** 对于  $f \in A$ , 有  $[u, \varphi]f = [\rho(\hat{f})u, \varphi]$ .

$$\begin{aligned} \text{証明 } ([u, \varphi]f)(x) &= \sum_{y \in G} [u, \varphi](xy)f(y^{-1}) \\ &= \sum_{y \in G} f(y^{-1})(\rho(x)\rho(y)u, \varphi) \\ &= \sum_{y \in G} f(y^{-1})(\rho(y)u, {}^t(\rho(x))\varphi) \\ &= (\rho(\hat{f})u, {}^t(\rho(x))\varphi) \\ &= (\rho(x)\rho(\hat{f})u, \varphi). \quad (\text{証毕}) \end{aligned}$$

假如对于張量积  $V \otimes \hat{V} \ni u \otimes \varphi$ , 使  $\mathfrak{L}(V)$  中把  $v \in V$  映射于  $\varphi(v)u = (v, \varphi)u \in V$  的元对应, 那就得到自  $V \otimes \hat{V}$  到  $\mathfrak{L}(V)$  上作为向量空間的同构映射, 这事实容易得知。由这对应, 如果把  $V \otimes \hat{V}$  与  $\mathfrak{L}(V)$  同样看待, 就有下面的命题。

**命题 52** 对于  $\tau \in GL(V)$ ,  $u \in V$ ,  $\varphi \in \hat{V}$ , 有

$$\tau \circ (u \otimes \varphi) = (\tau u) \otimes \varphi.$$

**証明** 对于任意  $v \in V$ ,

$$(\tau \circ (u \otimes \varphi))(v) = \tau((v, \varphi)u) = (v, \varphi)\tau u = ((\tau u) \otimes \varphi)(v).$$

**命题 53**  $\tau - \sum_{x \in G} (\rho(x) u \otimes \varphi) \cdot \rho(x^{-1}) \in Z,$

**证明** 对于任意  $y \in G,$

$$\begin{aligned} \rho(y) \tau \rho(y^{-1}) &= \sum_{x \in G} (\rho(yx) u \otimes \varphi) \rho(x^{-1} y^{-1}) \\ &= \sum_{z \in G} (\rho(z) u \otimes \varphi) \rho(z^{-1}) = \tau. \quad (\text{証毕}) \end{aligned}$$

以下假定  $A$  的左理想全体的集合是  $\mathfrak{M}$ ,  $\mathfrak{M}$  中元一般用  $M$  表示, 对  $Z$  不变的子空间全体的集合是  $\mathfrak{W}$ ,  $\mathfrak{W}$  中元一般用  $W$  表示, 依照 Weyl 引入下面的记法:

$${}^{\#}M = \{u; \forall \varphi \in \hat{V}, [u, \varphi] \in M\}, \quad (42.2)$$

$$\begin{aligned} {}^{\#}W = \left\{ f; f = \sum_{i=1}^m [u_i, \varphi_i], u_i \in W, \varphi_i \in \hat{V} \right\} \\ (m=1, 2, \dots), \quad (42.3) \end{aligned}$$

这里  $u, f$  当然分别是  $V, A$  中元。

**命题 54** (i)  ${}^{\#}M \in \mathfrak{M}$ , (ii)  ${}^{\#}W \in \mathfrak{W}$ .

(iii)  $M \supset M' \Rightarrow {}^{\#}M \supset {}^{\#}M'$ .

(iv)  $W \supset W' \Rightarrow {}^{\#}W \supset {}^{\#}W'$ . 特别  ${}^{\#}V \supset {}^{\#}W$ .

**证明** (i) 取任意  $\zeta \in Z, u \in {}^{\#}M$ , 证明  $\zeta(u) \in {}^{\#}M$ , 即  $\forall \varphi \in \hat{V}, [\zeta(u), \varphi] \in M$  即可。因为

$$\begin{aligned} [\zeta(u), \varphi](x) &= \varphi(\rho(x) \circ \zeta(u)) = \varphi(\zeta \circ \rho(x)(u)) \\ &= {}^t\zeta \circ \varphi(\rho(x)(u)) = [u, {}^t\zeta \circ \varphi](x), \end{aligned}$$

所以  $[\zeta(u), \varphi] = [u, {}^t\zeta \circ \varphi]$ . 但  $u \in {}^{\#}M$ , 所以它  $\in M$ .

(ii)  ${}^{\#}W$  成为  $A$  的子空间是明显的。更对于任意

$$x \in G, {}^{\#}W \ni f = \sum_{i=1}^m [u_i, \varphi_i] \quad (u_i \in W),$$

$$\begin{aligned} \text{因为 } (xf)(y) &= f(x^{-1}y) \text{ ①} = \sum_{i=1}^m (\rho(x^{-1}y) u_i, \varphi_i) \\ &= \sum_{i=1}^m (\rho(y) u_i, {}^t\rho(x^{-1}) \varphi_i) = \sum_{i=1}^m [u_i, {}^t\rho(x^{-1}) \varphi_i](y), \end{aligned}$$

① 因为  $(xf)(y) = (f_x \cdot f)(y) = \sum_{z \in G} f_x(yz^{-1})f(z)$ . 而  $f_x(yz^{-1})$  仅当  $x = yz^{-1}$ , 即  $z = x^{-1}y$  时不为 0, 其他都为 0, 所以  $(xf)(y) = f(x^{-1}y)$ . ——译者注

所以  $xf = \sum_{i=1}^n [v_i, {}^t\rho(x^{-1})\varphi_i] \in {}^tW$ .

因此  ${}^tW \in \mathfrak{M}$ .

(iii), (iv) 由定义自明。 (証毕)

一般, 有  $(C$  上) 向量空間  $V$  的子集合  $M$  时, 由  $M$  生成的  $V$  的子空間  $[M]$  叫做  $M$  的綫性包絡 (linear envelope, lineare Hülle)。自  $M$  到又一向量空間  $V'$  中的映射  $f$  如果滿足条件:

$$\sum_{i=1}^k \lambda_i x_i = 0 \Rightarrow \sum_{i=1}^k \lambda_i f(x_i) = 0 \quad (\lambda_i \in C, x_i \in M, k=1, 2, \dots),$$

命

$$\tilde{f}\left(\sum_{i=1}^r \mu_i x_i\right) = \sum_{i=1}^r \mu_i f(x_i) \quad (\mu_i \in C, x_i \in M, r=1, 2, \dots),$$

那就容易理解  $\tilde{f} \in \mathfrak{L}([M], V')$ 。  $\tilde{f}$  叫做  $f$  的綫性擴張, 通常用同一文字  $f$  表示。显然  $f([M]) = [f(M)]$ .

例3  $\mathfrak{L}(V)$  是  $GL(V)$  的綫性包絡 (让讀者考虑)。

例4  $A = A(G)$  是  $G$  的綫性包絡, 在 181 頁例5 中定义的  $\rho$  是对应于它的綫性擴張。

一般, 假定  $S$  是一个代数系 (群, 代数等, 但考虑代数时, 基础体假定是  $C$ ),  $V$  是  $(C$  上) 向量空間,  $\rho$  是自  $S$  到  $\mathfrak{L}(V)$  中的同态映射。这时  $\rho$  叫做在  $V$  中  $S$  的表現,  $V$  叫做它的表現空間。 $S$  的子集合  $S_0$  及它的表現  $\rho_0$  給定时, 假如  $S$  是  $S_0$  的綫性包絡, 那就能够得到作为  $\rho_0$  的綫性擴張的  $S$  的表現  $\rho$ 。

假定  $\rho_1, \rho_2$  是  $S$  的两个表現, 它們的表現空間分別是  $V_1, V_2$ , 而

$$\begin{array}{ccc} V_1 & \xrightarrow{\rho_1(x)} & V_1 \\ \phi \downarrow & & \downarrow \phi \\ V_2 & \xrightarrow{\rho_2(x)} & V_2 \end{array} \quad \begin{array}{l} \Phi \text{ 是自 } V_1 \text{ 到 } V_2 \text{ 作为向量空間的同构映射, 当} \\ \forall x \in S, \rho_2(x) \circ \Phi = \Phi \circ \rho_1(x) \\ \text{时 (与群的表現情况同样), } \rho_1 \text{ 与 } \rho_2 \text{ 叫做等价,} \\ V_1 \text{ 与 } V_2 \text{ 叫做作为 } S \text{ 的表現空間同构。写成} \end{array}$$

$\rho_1 \sim \rho_2, V_1 \sim V_2$ , 不变子空間的概念也与群表現时的同样定义, 即

代数系  $S$  的表现  $\rho$  的表现空间  $V$  的子空间  $W$ , 如果是  $\mathfrak{U}(V)$  集合  $\rho(S)$  的不变子空间 (168 页),  $W$  叫做  $V$  的  $S$ -不变子空间。

**例 5** 假定  $S$  是  $\mathfrak{U}(V)$  集合又成为一个代数系。这时  $\rho(x) = x, x \in S$  的表现  $\rho$  给出  $S$  的同构表现, 它叫做  $S$  的自然表现。

**例 6** 假定  $S$  与例 3 同样, 如果取  $V$  的  $S$ -不变子空间  $W_1, W_2$ , 那就得到  $\rho_i(x) = x|W_i$  的表现  $\rho_i (i=1, 2)$ , 为了  $\rho_1 \sim \rho_2$  或  $W_1 \sim W_2$ , 下面的条件是必要充分的: 存在满足  $\forall x \in S, \forall u \in W_1, x \circ \varphi(u) = \varphi \circ x(u)$  这样自  $W_1$  到  $W_2$  作为向量空间的同构映射  $\varphi$ 。

假定  $\mathfrak{M}$  的元中, 含于  ${}^bV$  的全体集合是  $\mathfrak{M}_0$ <sup>①</sup>, 那末由命题 54 (iv) 得  ${}^bW \in \mathfrak{M}_0$ 。因为  $\mathfrak{M}$  中元 (因而当然  $\mathfrak{M}_0$  中元) 都是  $G$  的左正则表现的表现空间, 所以  $A$  也是它的线性扩张表现的表现空间。又因为  $\mathfrak{M} \ni W$  是  $Z$ -不变子空间, 所以存在把  $W$  作为表现空间  $\rho(\zeta) = \zeta|W, \zeta \in Z$ , 这样代数  $Z$  的表现。

**Weyl 的相互律** 是表示在作为表现空间的集合  $\mathfrak{M}, \mathfrak{M}_0$  之间, 根据 #,  $\sharp$  有保存作为表现空间同构关系的一对一的对应, 即下面的定理成立。

**定理 33 (Weyl)** 假定  $A$  是有限群  $G$  的群代数,  $\rho$  是  $G$  的表现,  $V$  是  $\rho$  的表现空间,  $Z$  是  $\rho(G) (\subset GL(V))$  的交换子代数。把  $A$  的左理想集合作为  $\mathfrak{M}$ ,  $V$  的  $Z$ -不变子空间的集合作为  $\mathfrak{M}$ 。对于  $u \in V, \varphi \in \hat{V}$ , 由 (42.1) 定义  $[u, \varphi] \in A$ , 对于  $M \in \mathfrak{M}, W \in \mathfrak{M}$ , 由 (42.2), (42.3) 定义  ${}^*M, {}^bW$ 。又假定  $\mathfrak{M}$  的元中含于  ${}^bV$  的集合是  $\mathfrak{M}_0$ , 那末对于  $M, M' \in \mathfrak{M}_0, W, W' \in \mathfrak{M}$ ,

- (i)  ${}^{**}M = M, (ii) {}^{**}W = W,$
- (iii)  ${}^*(M \oplus M') = {}^*M \oplus {}^*M', {}^b(W \oplus W') = {}^bW \oplus {}^bW',$
- (iv)  $M \sim M' \Leftrightarrow {}^*M \sim {}^*M', W \sim W' \Leftrightarrow {}^bW \sim {}^bW'.$

<sup>①</sup> 因为一般  ${}^bV \subset A(G)$ , 但可能  ${}^bV \neq A(G)$ , 又由命题 54,  ${}^bV$  是  $A(G)$  的左理想, 所以它含有  $A(G)$  中的左理想, 但不一定包含  $A(G)$  中所有左理想。——译者注

这定理的証明在本质上是引用上面諸命题，再把下面三个引理作为准备。首先注意由 § 37 命题 20,  $\mathfrak{M}$  中元  $M$  能够用  $A$  中适当幂等元  $\varepsilon$  写成  $A\varepsilon$  的形状。

**引理 1** 假定把  $\mathfrak{M}$  中任意元  $M$  写成  $M = A\varepsilon$  ( $\varepsilon$  是幂等元), 那末

$${}^*M = \rho(\hat{\varepsilon})V.$$

**証明** 由下面的关系显然。

$$\begin{aligned} u \in {}^*M &\Leftrightarrow \forall \varphi \in \hat{V}, [u, \varphi] \in M \\ &\Leftrightarrow \forall \varphi \in \hat{V}, [u, \varphi]\varepsilon = [u, \varphi] \quad (\text{由 230 頁命题 20 上 2 行}) \\ &\Leftrightarrow \forall \varphi, [\rho(\hat{\varepsilon})u, \varphi] = [u, \varphi] \quad (\text{由命题 51}) \\ &\Leftrightarrow \rho(\hat{\varepsilon})u = u \quad (\text{由命题 49}) \\ &\Leftrightarrow u \in \rho(\hat{\varepsilon})V \quad (\text{由 } \Leftarrow u = \rho(\hat{\varepsilon})V \Rightarrow \rho(\hat{\varepsilon})u = u). \end{aligned}$$

**引理 2**  ${}^{**}M \subset M$ ,  ${}^*{}^*W \supset W$ .

**証明** 由定义自明。

**引理 3**  ${}^*V$  是两侧理想。

**証明**  ${}^*V$  当然是左理想。在証明它又是右理想时, 証明对于任意  $f \in A$ ,  ${}^*V \cdot f \subset {}^*V$  即可。假定

$${}^*V \ni g = \sum_{i=1}^m [u_i, \varphi_i], \quad u_i \in V,$$

那末 
$$gf = \sum_{i=1}^m [u_i, \varphi_i]f = \sum_{i=1}^m [\rho(\hat{f})u_i, \varphi_i].$$

这里当然  $\rho(\hat{f})u_i \in V$ , 所以  $gf \in {}^*V$ .

**定理 33 的証明** (i) 假如用幂等元  $\varepsilon$  写成  $M = A\varepsilon$ , 因为  $M \subset {}^*V$ , 所以  $f \in M$  能够写成

$$f = f\varepsilon = \sum_{i=1}^m [u_i, \varphi_i]\varepsilon = \sum_{i=1}^m [\rho(\hat{\varepsilon})u_i, \varphi_i], \quad u_i \in V.$$

由引理 1,  $\rho(\hat{\varepsilon})u_i \in \rho(\hat{\varepsilon})V = {}^*M$ , 所以  $f \in {}^{**}M$ . 因此  $M \subset {}^{**}M$ . 由这与引理 2 即得到  $M = {}^{**}M$ .

(ii) 假如用幂等元  $\varepsilon$  写成  ${}^*W = A\varepsilon$ , 那末由引理 1,  ${}^{**}W = \rho(\hat{\varepsilon})V$ . 因此

$$\rho(\hat{\varepsilon}) = \sum_{x \in G} \hat{\varepsilon}(x^{-1}) \rho(x^{-1}) = \sum_{x \in G} \varepsilon(x) \rho(x^{-1}).$$

又因为  $\varepsilon \in {}^*W$ , 所以

$$\varepsilon(x) = \sum_{i=1}^m [\psi_i, \varphi_i](x) = \sum_{i=1}^m (\rho(x) \psi_i, \varphi_i), \quad \psi_i \in W.$$

于是(用引理 1 的证明中最后行)

$$\begin{aligned} {}^*W \ni v &= \rho(\hat{\varepsilon})v = \sum_{i=1}^m \sum_{x \in G} (\rho(x) \psi_i, \varphi_i) \rho(x^{-1})v \\ &= \sum_{i=1}^m \sum_{x \in G} (\rho(x^{-1})v \otimes \varphi_i) \rho(x) \psi_i. \end{aligned}$$

但由命题 53,  $\sum_{x \in G} (\rho(x^{-1})v \otimes \varphi_i) \rho(x) \in Z$ . 由这与  $\psi_i \in W$  得

$$\sum_{x \in G} (\rho(x^{-1})v \otimes \varphi_i) \rho(x) \psi_i \in W.$$

所以  $v \in W$ . 因此  ${}^{**}W \subset W$ . 由这与引理 2 即得  ${}^{**}W = W$ .

(iii) 因为  $M, M' \subset M \oplus M'$ , 所以  ${}^*M, {}^*M' \subset {}^*(M \oplus M')$ . 因此  ${}^*M \oplus {}^*M' \subset {}^*(M \oplus M')$ . 再因为  ${}^*M, {}^*M' \subset {}^*M \oplus {}^*M'$ , 所以  $M, M' \subset {}^*({}^*M \oplus {}^*M')$ . 因此  $M \oplus M' \subset {}^*({}^*M \oplus {}^*M')$ . 于是  ${}^*(M \oplus M') \subset {}^*M \oplus {}^*M'$ . 所以

$${}^*(M \oplus M') = {}^*M \oplus {}^*M'.$$

同样

$${}^*(W \oplus W') = {}^*W \oplus {}^*W'.$$

对于 (iv), 证明  $M \sim M' \Rightarrow {}^*M \sim {}^*M', W \sim W' \Rightarrow {}^*W \sim {}^*W'$  两条即可。

假定  $M \sim M'$ . 由命题 22 系 2,  $M$  与  $M'$  之间的同构对应能够用适当的  $f_0, f'_0 \in A$ , 由

$$f' = ff_0, f = f'_0 f' \quad (f \in M, f' \in M')$$

给出, 对于所有的  $f \in M$  有  $f = ff_0 f'_0$ . 现在假定  $u \in {}^*M$ , 那末

$\forall \varphi \in \hat{V}$ ,  $[u, \varphi] \in M$ . 于是  $\forall \varphi$ ,  $[\rho(\hat{f}_0)u, \varphi] = [u, \varphi]f_0 \in M'$ . 所以  $\rho(\hat{f}_0)u \in {}^*M'$ . 因此假如对于  $u$ , 使  $\rho(\hat{f}_0)u$  对应的映射是  $\Phi: {}^*M \rightarrow {}^*M'$ , 那末来証明  $\Phi$  給出自  ${}^*M$  到  ${}^*M'$  的同构映射。与  $\Phi$  同样,  $\Psi: {}^*M' \rightarrow {}^*M$ , 由  $\Psi(u') = \rho(\hat{f}'_0)u' (u' \in {}^*M')$  定义,

$$\begin{aligned} \forall \varphi, [\Psi\Phi(u), \varphi] &= [\rho(\hat{f}'_0)\rho(\hat{f}_0)u, \varphi] = [\rho(\widehat{f'_0 f_0})u, \varphi] \\ &= [u, \varphi]f_0 f'_0 = [u, \varphi]. \end{aligned}$$

所以由命题 49,  $\Psi\Phi(u) = u$ . 同样  $\Phi\Psi(u') = u'$ . 因此由 28 頁例 10,  $\Phi, \Psi$  是全单射且互为逆映射, 并且显然  $\Phi$  是綫性映射。又对于任意  $\zeta \in Z$ , 因为  $\zeta\Phi = \Phi\zeta$ , 所以  $\Phi$  給出自  ${}^*M$  到  ${}^*M'$  作为表現空間的同构映射。因此  ${}^*M \sim {}^*M'$ .

其次, 假定  $W \sim W'$ . 即有自  $W$  到  $W'$  的同构对应  $\Phi$ , 对于任意  $\zeta \in Z$ , 假定  $\zeta\Phi = \Phi\zeta$ . 这时对于

$${}^*W \ni f = \sum_{i=1}^m [u_i, \varphi_i] \quad (u_i \in W, \varphi_i \in \hat{V}),$$

如果 
$$g = \sum_{i=1}^m [\Phi(u_i), \varphi_i],$$

显然  $g \in {}^*W'$ , 但由对于  $f$  使与  $g$  对应能够得到  ${}^*W$  与  ${}^*W'$  之間作为表現空間的同构对应, 这事实示明如下。

首先, 示明不論  $f$  的表示方法如何,  $g$  对于  $f$  是唯一地确定。为此証明  $f=0 \Rightarrow g=0$  即可。假定  $u \in V$ , 如果命

$$\tau_i(u) = \sum_{x \in G} (\rho(x)u \otimes \varphi_i) \rho(x^{-1}),$$

那末

$$\begin{aligned} \rho(\hat{f})u &= \sum_{x \in G} f(x^{-1}) \rho(x)u = \sum_{x \in G} \sum_{i=1}^m (\rho(x^{-1})u_i, \varphi_i) \rho(x)u \\ &= \sum_{i=1}^m \sum_{x \in G} (\rho(x)u \otimes \varphi_i) \rho(x^{-1})u_i = \sum_{i=1}^m \tau_i(u) u_i. \end{aligned}$$

假如命  $\Phi(u_i) = v_i$ , 同样得

$$\rho(\hat{g})u = \sum_{i=1}^m \tau_i(u) u_i.$$

由命題 53, 因为  $\tau_i(u) \in Z$ , 所以

$$\rho(\hat{g})u = \sum_{i=1}^m \tau_i(u) \Phi(u_i) = \sum_{i=1}^m \Phi \tau_i(u) u_i = \Phi(\rho(\hat{f})u).$$

因此  $f=0 \Rightarrow \forall u \in V, \rho(\hat{f})u=0$

$$\Rightarrow \forall u \in V, \rho(\hat{g})u=0$$

$$\Rightarrow \forall u \in V, \forall \varphi \in \hat{V}, [\rho(\hat{g})u, \varphi] = [u, \varphi]g = 0.$$

因为  ${}^1V$  中元能够表示为  $\sum_{i=1}^m [u_i, \varphi_i]$ ,  $u_i \in V, \varphi_i \in \hat{V}$  形状, 所以如果  $f=0$ , 那末  ${}^1V \cdot g = 0$ . 由引理 3 有满足  ${}^1V \ni \varepsilon, \forall h \in {}^1V, \varepsilon h = h$  的幂等元  $\varepsilon$ . 因此  $g = \varepsilon g = 0$ .

假定由以上所定义的自  ${}^1W$  到  ${}^1W'$  的映射是  $\Phi'$ , 与前半段同样考察, 得知  $\Phi'$  是全单射. 又  $\Phi'$  显然是綫性映射. 对于任意  $x \in G, f \in W$ ,

$$\begin{aligned} \Phi'x(f) &= \Phi'x\left(\sum_{i=1}^m [u_i, \varphi_i]\right) \\ &= \sum_{i=1}^m \Phi'(x[u_i, \varphi_i]) \quad (u_i \in W, \varphi_i \in \hat{V}) \\ &= \sum_{i=1}^m \Phi'([u_i, {}^t\rho(x^{-1})\varphi_i]) \quad (\text{命題 50}) \\ &= \sum_{i=1}^m [v_i, {}^t\rho(x^{-1})\varphi_i] \\ &= x \sum_{i=1}^m [v_i, \varphi_i] = x\Phi'(f) \quad (v_i = \Phi(u_i) \in W'). \end{aligned}$$

因此  ${}^1W \sim {}^1W'$ .

系 把  $M \in \mathfrak{M}_0, W \in \mathfrak{W}$  分別看成  $G, Z = \mathfrak{C}(\rho(G))$  的表現空間时, 如果  $M$  是既約, 那末  ${}^*M$  也是既約. 又如果  $W$  是既約, 那末  ${}^1W$  也是既約.



## § 43 一般綫性变换群的張量表現

假定  $M$  是固定的自然数,  $V$  是  $C$  上  $m$  維向量空間。  $V$  的一般綫性变换群为  $\mathfrak{G} = GL(V)$ ,  $\mathfrak{G}$  当然是无限群。在本章直到現在只以討論有限群的表现为主, 在这最后一节来考虑无限群  $\mathfrak{G}$  的表现。

$\mathfrak{G}$  能够看成为它自身  $\mathfrak{G}$  的表现, 这是  $\mathfrak{G}$  的“自然表现” (§ 25, 例 3)。这自然表现用  $\sigma$  表示。  $n$  个  $\sigma$  的張量积  $\sigma \underset{\leftarrow n \uparrow}{\otimes} \cdots \underset{\leftarrow n \uparrow}{\otimes} \sigma = \sigma^n$ , 成为把  $m^n$  維向量空間  $V \otimes \cdots \otimes V = V^n$  作为表现空間的  $\mathfrak{G}$  的表现。  $\sigma^n$  叫做  $n$  阶的張量表现 (更由 264 頁  $\sigma^n$  也能够 在  $\mathfrak{G} = GL(V)$  的綫性包絡  $\mathfrak{L}(V)$  中定义。因此  $\sigma^n(\mathfrak{L}(V))$  也有意义)。如在 § 25, 例 6 中注意的那样,  $\sigma$  是  $\mathfrak{G}$  的既約表现, 但  $\sigma^n$  当然一般不是既約 (因为  $\mathfrak{G}$  不是有限群), 作为有限群表现論出发点的定理 8 在这里也不能使用。但应用前节定理 33, 張量表现  $\sigma^n$  是完全可約, 并且这既約表现的直和分解能够用  $n$  阶对称群  $G = \mathfrak{S}_n$  的表现理論求得。为了簡單起見, 以下固定取  $V$  的一个基底  $\{u_1, \cdots, u_m\}$ , 就由它用 127 頁的方法构成的  $V^n$  的基底  $\{u^{(1)}, \cdots, u^{(m^n)}\}$  ( $u^{(1)} = u_1 \underset{\leftarrow n \uparrow}{\otimes} \cdots \underset{\leftarrow n \uparrow}{\otimes} u_1$ ,  $u^{(2)} = u_1 \underset{\leftarrow (n-1) \uparrow}{\otimes} \cdots \underset{\leftarrow (n-1) \uparrow}{\otimes} u_1 \underset{\leftarrow n \uparrow}{\otimes} u_2, \cdots, u^{(m^n)} = u_m \underset{\leftarrow n \uparrow}{\otimes} \cdots \underset{\leftarrow n \uparrow}{\otimes} u_m$ ) 来討論。

首先对于  $G = \mathfrak{S}_n \ni x$  定义  $\rho(x) \in GL(V^n)$  如下:

对于  $V^n$  的基底  $u^{(i)} = u_{j_1} \otimes \cdots \otimes u_{j_n}$ ,

$$\rho(x) u^{(i)} = u_{j_{x(1)}} \otimes \cdots \otimes u_{j_{x(n)}},$$

对于  $V^n$  的一般元  $v = \sum_{i=1}^{m^n} \lambda^{(i)} u^{(i)}$ ,

$$\rho(x) v = \sum_{i=1}^{m^n} \lambda^{(i)} \rho(x) u^{(i)}.$$

(43.1)

这样,  $\rho$  显然是  $G$  把  $V^n$  作为表现空間的表现。

例 1 假定  $m=4, n=3$ , 如果  $x = (132)$ , 那末

$$\rho(x)(u_1 \otimes u_2 \otimes u_3) = u_2 \otimes u_1 \otimes u_3.$$

一般, 假如

$$\mathfrak{S}_n \ni x = \begin{pmatrix} 1 & 2 & \cdots & n \\ \nu_1 & \nu_2 & \cdots & \nu_n \end{pmatrix},$$

那末

$$\rho(x)(u_{j_1} \otimes \cdots \otimes u_{j_n}) = u_{j_{\nu_1}} \otimes \cdots \otimes u_{j_{\nu_n}}.$$

**例 2** 假定  $\rho(x)u^{(i)} = u^{(i')}$ ,  $x$  是自然数  $i (1 \leq i \leq m^n)$  的函数, 对于  $i$  的值看成为  $i'$ . 这函数关系用

$$i' = x[i]$$

表示。即

$$\rho(x)u^{(i)} = u^{x[i]}.$$

又命

$$x = \begin{pmatrix} 1 & 2 & \cdots & n \\ \nu_1 & \nu_2 & \cdots & \nu_n \end{pmatrix} \text{ 时, } x(\mu) = \nu_\mu,$$

那末  $x(\mu)$  是定义于自然数  $\mu (1 \leq \mu \leq n)$  而与  $x[i]$  完全不同的函数。这函数  $x(\mu)$  在 (43.1) 已经引用。这记法  $x[i]$ ,  $x(\mu)$  在以下常常引用。

关于把上面那样定义的  $V^n$  作为表现空间的  $G$  的表现  $\rho$  与  $\mathfrak{S}$  的张量表现  $\sigma^n$  间的关系, 有下面重要的命题。

**命题 55** 假定  $\rho$  是在上面定义的  $G$  的表现, 如果  $\rho(G)$  的交换子代数  $\mathfrak{S}(\rho(G))$  是  $Z(\subset GL(V^n))$  时, 那末  $V^n$  的子空间  $W$  是  $Z$ -不变与  $W$  是  $\sigma^n(\mathfrak{S})$ -不变是同一回事。

$$\begin{array}{ccc} \mathfrak{S} = GL(V) & \xrightarrow{\sigma^n} & V^n \supset W \in \mathfrak{N} \\ & \nearrow \rho & \updownarrow \# \updownarrow \# \updownarrow \\ G = \mathfrak{S}_n & \xrightarrow[\text{正则表现}]{} & A \supset V^n \supset M \in \mathfrak{M}. \end{array}$$

今假定承认这命题, 如果把前节的  $G$ ,  $\rho$  分别作为是在上面所定义的, 那末前节的  $\mathfrak{N}$  能够看成为  $\mathfrak{S}$  的表现  $\sigma^n$  的表现空间的子表现空间的全体。这样由定理 33 (Weyl 的相互律),  $\mathfrak{S}$  的表现空间  $W$  与含于  $V^n$  的  $A = A(G)$  的左理想  $M$  之间一对一的对应成立,  $\mathfrak{S}$  的既约表现空间都能够自含于  $V^n$  的既约左理想  $M = Ac$  由作  $\#M = \rho(\hat{c})V$  的操作得出。又  $W_1, W_2 \in \mathfrak{N}$  是否是等价的表現空間, 由  $A(G)$  中对于它们的左理想  ${}^{\#}W_1, {}^{\#}W_2$ , 是否是等价来确

定。更有限群  $G$  的表現是完全可約。

因为  ${}^nV$  能够直和分解为

$${}^nV = M_1 \oplus \cdots \oplus M_k,$$

( $M_i, i=1, \dots, k$  是  $A(G)$  的既約左理想)

形状, 所以对于它的  $\sigma^n$  的表現空間也能够分解为既約表現空間的直和

$$V^n = {}^*M_1 \oplus \cdots \oplus {}^*M_k.$$

因此得知  $\sigma^n$  是完全可約的。又  ${}^*M_i$  在  $V^n$  的重复度显然与  $M_i$  在  ${}^nV$  的重复度一致。因为关于  $G = \mathfrak{S}_n$  的表現在 §38~§41 已詳叙, 所以利用它能够解决关于  $\sigma^n$  同种类的問題。对于这些結果汇集作为后面的定理 34 来叙述。再判別  $A(G)$  的既約左理想含于  ${}^nV$  与否的問題是新发生的, 但它也能够用  $G = \mathfrak{S}_n$  的台来简单的解决。这事实也在定理 34 中叙述, 証明也在那里給出。

其次, 为了証明命題 55 及定理 34 需准备两个必要概念和几个引理。

对于  $G$  的子群  $H$ , 把滿足  $V^n \supset v, \forall x \in H, \rho(x)v = v$  的, 叫做  $n$  阶关于  $H$  的对称張量, 把滿足  $V^n \supset w, \forall x \in H, \rho(x)w = (\text{sgn } x)w$  的, 叫做  $n$  阶关于  $H$  的反对称張量。当  $H = G$  时“关于  $G$ ”这語省略。

$n$  阶的对称張量全体  $S^n$ , 反对称張量全体  $S'^n$  显然分別构成  $V^n$  的子向量空間。

**例 3**  $m=2, n=2$  时,  $V^n = V^2$  的基底由  $u^{(1)} = u_1 \otimes u_1, u^{(2)} = u_1 \otimes u_2, u^{(3)} = u_2 \otimes u_1, u^{(4)} = u_2 \otimes u_2$  四个元构成, 它們中  $u^{(1)}, u^{(4)} \in S^2$ . 又因为  $\rho(1\ 2)u^{(2)} = u^{(3)}$ , 所以由  $u^{(i)}$  的无关性,  $\sum_{i=1}^4 \lambda^{(i)} u^{(i)} \in S^2 \Leftrightarrow \lambda^{(2)} = \lambda^{(3)}$ . 因此  $u^{(1)}, u^{(2)} + u^{(3)}, u^{(4)}$  三个元构成  $S^2$  的基底。一般, 对于  $V^n$  的基底  $u^{(i)} = u_{j_1} \otimes \cdots \otimes u_{j_n}$ , 如果命  $\sum_{x \in G} \rho(x) u^{(i)} = S(u^{(i)})$ , 在  $j_1, \dots, j_n$  中假如 1 有  $\mu_1^{(i)}$  个,  $\dots, m$  有  $\mu_m^{(i)}$  个 ( $\mu_1^{(i)} + \cdots + \mu_m^{(i)} = n$ ) 时, 那末  $S(u^{(i)}) = S(u^{(i')}) \Leftrightarrow \mu_1^{(i)} = \mu_1^{(i')}, \dots, \mu_m^{(i)}$

$-\mu_m^{(i)}$  ①, 总共做成  $\binom{n+m-1}{n}$  个  $S(u^{(i)})$  ② 它们构成  $S^n$  的基底是容易理解的。因此

$$\dim S^n = \binom{n+m-1}{n}.$$

**例 4**  $m=2, n=2$  时, 用与上同样记法, 那末  $S^n = S'^2$  的基底是  $u^{(2)} = u^{(3)}$ ,  $\dim S'^2 = 1$ . 一般, 假如  $V^n$  中元  $v = \sum \lambda^{(i)} u^{(i)} = \sum \lambda_{j_1 \dots j_n} u_{j_1} \otimes \dots \otimes u_{j_n} \in S'^n$ , 例如, 如果  $j_1 = j_2$ , 那末

$$\begin{aligned} \rho(1 \ 2) v &= \lambda_{j_1 j_1 \dots j_n} u_{j_1} \otimes u_{j_1} \otimes \dots \otimes u_{j_n} + \dots \\ &= \lambda_{j_1 j_1 \dots j_n} u_{j_1} \otimes u_{j_1} \otimes \dots \otimes u_{j_n} + \dots \\ &= -v = -\lambda_{j_1 j_1 \dots j_n} u_{j_1} \otimes \dots \otimes u_{j_n} + \dots, \end{aligned}$$

① 假如在  $\mu^{(i)}$  中有  $\mu_1^{(i)}$  个 1,  $\mu_2^{(i)}$  个 2,  $\dots$ ,  $\mu_m^{(i)}$  个  $m$ , 在  $\mu^{(i')}$  中有  $\mu_1^{(i')}$  个 1,  $\mu_2^{(i')}$  个 2,  $\dots$ ,  $\mu_m^{(i')}$  个  $m$ , 那末  $S(u^{(i)}) = S(u^{(i')})$ . 例如  $m=2, n=3, V^n = V'^3$ . 假设  $u^{(i)} = u_1 \otimes u_2 \otimes u_2, u^{(i')} = u_2 \otimes u_1 \otimes u_2$ , 则  $\mu_1^{(i)} = 1, \mu_2^{(i)} = 2, \mu_1^{(i')} = 1, \mu_2^{(i')} = 2$ , 此时

$$S = \sum_{x \in G} \rho(x) = \rho(1) + \rho(1 \ 2) + \rho(1 \ 3) + \rho(2 \ 3) + \rho(1 \ 2 \ 3) + \rho(1 \ 3 \ 2),$$

$$\begin{aligned} S(u^{(i)}) &= \sum_{x \in G} \rho(x)(u^{(i)}) = u_1 \otimes u_2 \otimes u_2 + u_2 \otimes u_1 \otimes u_2 + u_2 \otimes u_2 \otimes u_1 \\ &\quad + u_1 \otimes u_2 \otimes u_2 + u_2 \otimes u_2 \otimes u_1 + u_2 \otimes u_1 \otimes u_2, \end{aligned}$$

$$\begin{aligned} S(u^{(i')}) &= \sum_{x \in G} \rho(x)(u^{(i')}) = u_2 \otimes u_1 \otimes u_2 + u_1 \otimes u_2 \otimes u_2 + u_2 \otimes u_1 \otimes u_2 \\ &\quad + u_2 \otimes u_2 \otimes u_1 + u_2 \otimes u_2 \otimes u_2 + u_2 \otimes u_2 \otimes u_1. \end{aligned}$$

所以  $S(u^{(i)}) = S(u^{(i')})$ .

反之, 假如  $S(u^{(i)}) = S(u^{(i')})$ , 那末  $\mu_1^{(i)} = \mu_1^{(i')}, \dots, \mu_m^{(i)} = \mu_m^{(i')}$ , 这是因为  $u^{(i)}$  中含的个数  $\mu^{(i)}$  不因置换  $S$  而改变, 如果  $\mu_1^{(i)} \neq \mu_1^{(i')}$ , 那末  $u^{(i)}$  必不在上式中的右边出现, 并且当  $x \neq 1$  时  $u^{(i)} \neq \rho(x)u^{(i)}$ , 因此由等式  $S(u^{(i)}) = S(u^{(i')})$  可推出  $u^{(i)}$  可由其他基底  $u^{(j)}$  线性表示, 而这与假定相反。——译者注

②  $S(u^{(i)})$  显然是属于  $S^n$ , 反之, 如果  $u \in S^n$ , 那末  $u \in V^n$ , 因此  $u$  可以用基底  $u^{(i)}$  线性表示。假定

$$u = \lambda_1 u^{(1)} + \lambda_2 u^{(2)} + \dots + \lambda_p u^{(p)},$$

那末

$$S(u) = S(\lambda_1 u^{(1)} + \lambda_2 u^{(2)} + \dots + \lambda_p u^{(p)}) = \lambda_1 S(u^{(1)}) + \lambda_2 S(u^{(2)}) + \dots + \lambda_p S(u^{(p)}),$$

由假定  $S(u) = u$ , 所以

$$u = \lambda_1 S(u^{(1)}) + \lambda_2 S(u^{(2)}) + \lambda_p S(u^{(p)}).$$

因此  $S(u^{(1)}), \dots, S(u^{(p)})$  是  $S^n$  的基底。

又因为  $S(u^{(i)})$  的个数等于  $\mu_1 + \mu_2 + \dots + \mu_m = n$  中非负的整数解的个数, 把它记

因此  $\lambda_{j_1, \dots, j_n} = 0$ . 同样用例3的記法, 假如  $\mu_1^{(0)}, \dots, \mu_m^{(0)}$  中只要有一个  $> 1$ , 那末  $\lambda^{(0)} = 0$ . 特別, 假如  $m < n$ , 那末  $S^n = 0$ . 假如  $m = n$ , 那末  $\dim S^n = 1$ ,  $S^n$  的基底由下面的元給出:  $\sum_{x \in G} (\text{sgn } x) \rho(x) (u_1 \otimes \dots \otimes u_n)$ . 假如  $m > n$ , 那末  $\dim S^n = \binom{m}{n}$ ,  $S^n$  的基底当  $\{j_1, \dots, j_n\} \subset \{1, 2, \dots, m\}$  时, 由  $\sum_{x \in G} (\text{sgn } x) \cdot \rho(x) (u_{j_1} \otimes \dots \otimes u_{j_n})$  給出。

**引理1** 假定  $u \in V$ , 那末  $\underbrace{u \otimes \dots \otimes u}_{\leftarrow n \uparrow} \in S^n$ . 又  $S^n$  与  $\{u \otimes \dots \otimes u; u \in V\}$  的綫性包絡  $S_0^n$  一致。

**証明** 前半段及  $S^n \supset S_0^n$  是明显的。为了証明  $S^n \subset S_0^n$ , 考虑  $V^n$  的对偶空間  $\hat{V}^n$ , 在  $\hat{V}^n$  的元中与  $S^n, S_0^n$  直交的全体(在49頁的意义下是  $S^n, S_0^n$  的零化空間)分別用  $T^n, T_0^n$  表示。这时  $T^n \supset T_0^n$ , 即对

成  $N(m, n)$ , 那末它就等于  $(z_1 + z_2 + \dots + z_m)^n$  的展开式中所含  $z_1 \dots z_m$  的乘积的項数, 如果令  $z_1 + (z_2 + \dots + z_m) = z_1 + V$ , 并将  $(z_1 + V)^n$  按二項式展开, 再将  $V = z_2 + \dots + z_m$  展开就可以看出下面的等式是成立的

$$N(m, n) = N(m, n-1) + N(m-1, n). \quad (1)$$

上式中的  $N(m, n-1)$  是含  $z_1$  的項数,  $N(m-1, n)$  是不含  $z_1$  的項数。

又因为对于任意  $m$ ,  $N(m, 1) = m$ , 对于任意  $n$ ,  $N(1, n) = 1$ . 因此在(1)式中如果令  $m=2$ , 就得到

$$N(2, n) = 1 + N(2, n-1),$$

同样

$$N(2, n-1) = 1 + N(2, n-2),$$

因为

$$N(2, 1) = 2,$$

所以从上面諸式即得  $N(2, n) = n+1$ .

再在(1)式中令  $m=3$  就有

$$N(3, n) = N(3, n-1) + N(2, n),$$

同样

$$N(3, n-1) = N(3, n-2) + N(2, n-1),$$

.....

$$N(3, 2) = N(3, 1) + N(2, 1),$$

$$N(3, 1) = 3.$$

由以上諸式即得

$$N(3, n) = \frac{1}{2} (n+1)(n+2).$$

一般由(1)对于  $m$  用数学归纳法即得

$$N(m, n) = \frac{(m+n-1)!}{(m-1)!n!} = \binom{n+m-1}{n}. \quad \text{——譯者注}$$

于  $\varphi \in \hat{V}^n$  証明  $(\forall u \in V, \varphi(u \otimes \cdots \otimes u) = 0 \Rightarrow \forall v \in S^n, \varphi(v) = 0)$  即可。因为象在例 3 所示的那样, 能够取  $S(u^{(i)})$  作为  $S^n$  的基底, 所以  $\forall v \in S^n, \varphi(v) = 0 \Leftrightarrow \forall i, \varphi(S(u^{(i)})) = 0$ . 今假定

$$u = \sum_{j=1}^m \lambda_j u_{j_1}$$

那末  $u \otimes \cdots \otimes u = \sum \lambda_{j_1} \lambda_{j_2} \cdots \lambda_{j_n} u_{j_1} \otimes \cdots \otimes u_{j_n}$ ,

因此, 假如  $\forall u \in V, \varphi(u \otimes \cdots \otimes u) = 0$ , 那末

$$\sum \lambda_{j_1} \lambda_{j_2} \cdots \lambda_{j_n} \varphi(u_{j_1} \otimes \cdots \otimes u_{j_n}) = 0$$

对于  $\forall \lambda_j \in \mathbb{C}$  成立。于是  $j_\nu$  独立变动于  $\{1, 2, \dots, m\}$ ,  $\sum$  就取  $m^n$  个项。命  $u^{(i)} = u_{j_1} \otimes \cdots \otimes u_{j_n}$ ,  $u^{(i')} = u_{j_1} \otimes \cdots \otimes u_{j_n}$ , 用例 3 的记法, 如果  $\mu_1^{(i)} = \mu_1^{(i')} = \mu_1, \dots, \mu_m^{(i)} = \mu_m^{(i')} = \mu_m$ , 那末

$$\lambda_{j_1} \lambda_{j_2} \cdots \lambda_{j_n} = \lambda_{j_1} \lambda_{j_2} \cdots \lambda_{j_n} = \lambda_1^{\mu_1} \lambda_2^{\mu_2} \cdots \lambda_m^{\mu_m}.$$

上面  $m^n$  个项的和整理为  $\binom{m+n-1}{n}$  项的和

$$\sum_{\mu_1 + \dots + \mu_m = n} \lambda_1^{\mu_1} \cdots \lambda_m^{\mu_m} \varphi(S(u_1 \otimes \cdots \otimes u_1 \otimes \cdots \otimes u_m \otimes \cdots \otimes u_m)).$$

$\xleftarrow{\mu_1 \uparrow} \qquad \qquad \qquad \xleftarrow{\mu_m \uparrow}$

这最后式子假如对于所有的  $\lambda_j \in \mathbb{C}, j=1, \dots, m$  是 0, 显然

$$\forall i \varphi(S(u^{(i)})) = 0 \text{ ①.}$$

**引理 2** 假定  $G = \mathfrak{S}_n$  的盘  $B$  的垂直置换构成的群是  $\mathfrak{R}$ ,  $B$  的 Young 的对称子是  $c$ , 那末  $\rho(\hat{c})V^n$  中元是关于  $\mathfrak{R}$  的反对称张量。

**証明** 由 261 页例 2,  $\hat{c} = KH$ . 因此, 如果  $k \in \mathfrak{R}, v \in V^n$ , 那末  $\rho(k)\rho(\hat{c})v = \rho(kKH)v = (\text{sgn } k)\rho(KH)v = (\text{sgn } k)\rho(\hat{c})v$ .

① 因为  $\varphi(S(\underbrace{u_1 \otimes \cdots \otimes u_1}_{\mu_1 \uparrow} \otimes \cdots \otimes \underbrace{u_m \otimes \cdots \otimes u_m}_{\mu_m \uparrow}))$  都是常数, 而  $\lambda_1, \dots, \lambda_m$  是  $\mathbb{C}$  中任意数, 所以

$$\sum_{\mu_1 + \dots + \mu_m = n} \lambda_1^{\mu_1} \cdots \lambda_m^{\mu_m} \varphi(S(\underbrace{u_1 \otimes \cdots \otimes u_1}_{\mu_1 \uparrow} \otimes \cdots \otimes \underbrace{u_m \otimes \cdots \otimes u_m}_{\mu_m \uparrow})),$$

可以看成  $\mathbb{C}$  上  $n$  次  $m$  个变量的多项式, 由多项式理论只有  $\varphi(S(u_1 \otimes \cdots \otimes u_1 \otimes \cdots \otimes u_m \otimes \cdots \otimes u_m))$  全为零时, 它才恒等于 0. ——译者注

所以  $\rho(\hat{c})v$  是关于  $\mathfrak{H}$  的反对称張量。 (証毕)

$\mathfrak{L}(V^n)$  中元对于上面固定的基底能够用  $m^n$  級方陣  $(\alpha_{ij}^{(v)}) = (\alpha_{i_1 \dots i_n, j_1 \dots j_n}^{(v)})$  表示。 $\alpha_{ij}^{(v)}$  表示它的第  $i$  行第  $j$  列的元素,  $V^n$  的基底中第  $i$  个, 第  $j$  个的元分别是  $u_{j_1} \otimes \dots \otimes u_{j_n}$ ,  $u_{i_1} \otimes \dots \otimes u_{i_n}$  时,  $\alpha_{ij}^{(v)}$  也写成  $\alpha_{i_1 \dots i_n, j_1 \dots j_n}^{(v)}$ . 以下考虑  $\mathfrak{L}(V^n)$  中元的矩陣表現时, 常常自开始固定的基底来考虑, 所以这事实不再一一声明。又把它矩陣表現与  $\mathfrak{L}(V^n)$  中元自身同样看待, 而写成  $\mathfrak{L}(V^n) \ni v = (\alpha_{ij}^{(v)})$ .

例5  $x \in G$  时, 表示  $\rho(x)$  的矩陣是第  $x[i]$  行, 第  $i$  列 ( $i=1, \dots, m^n$ ) 是 1, 其他元素都是 0 的矩陣。即

$$\rho(x) = \sum_{i=1}^{m^n} E_{x[i], i} \mathbf{1}.$$

上面作了把  $V^n$  作为表現空間的  $G$  的表現  $\rho(x)$ , 由它把  $\mathfrak{L}(V^n)$  作为表現空間的  $G$  的表現  $\tilde{\rho}(x)$  可如下来定义。即  $\rho(x)$  对于  $V^n$  的基底  $w^{(i)}$  由  $\rho(x)w^{(i)} = w^{(x[i])}$  来定义, 对于  $V^n$  的一般元成为它的綫性擴張。 $\mathfrak{L}(V^n)$  有  $m^{2n}$  个基底  $E_{i,l}$ ,  $\mathfrak{L}(V^n)$  中一般元  $(\alpha_{ij}^{(v)})$  ( $m^n$  級矩陣) 能够写成  $\sum \alpha_{ij}^{(v)} E_{i,l}$ . 于是  $\tilde{\rho}$  对于  $E_{i,l}$  定义为

$$\tilde{\rho}(x) E_{i,l} = E_{x[i], x[l]} \textcircled{2},$$

对一般的元, 作为它的綫性擴張。它給出  $G$  的表現是明显的。

$\mathfrak{L}(V^n)$  中元  $\alpha_{ij}^{(v)}$  满足  $\forall x \in G, \tilde{\rho}(x)(\alpha_{ij}^{(v)}) = (\alpha_{ij}^{(v)})$  的, 即满足

$$\forall x \in G, \forall i, l \quad \alpha_{il}^{(v)} = \alpha_{x[i]x[l]}^{(v)}$$

的叫做双对称。假如  $\mathfrak{L}(V^n)$  的元中双对称的全体用  $\mathfrak{S}^n$  表示, 由引理 1 即得下面引理。

① 由  $\rho(v) = \sum_{i=1}^{m^n} E_{x[i], i}$  得知

$$\rho^{-1}(x) = \sum_{i=1}^{m^n} E_{i, x[i]}, \text{——譯者注}$$

② 这就是把  $\mathfrak{L}(V^n)$  看成向量空間,  $\tilde{\rho}(x)$  是这向量空間的綫性变换。——譯者注

**引理 3**  $\tilde{S}^n$  与  $\sigma^n(\mathfrak{G})$  ( $\subset GL(V^n)$ ) 的綫性包絡一致<sup>①</sup>。

**証明** 在引理 1, 如果把  $V$  用  $\mathfrak{L}(V)$  ( $\cong V \otimes \hat{V}$ ) 替换 (注意  $\mathfrak{L}(V^n) \cong (\mathfrak{L}(V))^n$ ) 就得到  $\tilde{S}^n = [\sigma^n(\mathfrak{L}(V))]$ . 这右边由 264 頁命題 54 証明的后面得

$$[\sigma^n([\mathfrak{G}])] = [[\sigma^n(\mathfrak{G})]] = [\sigma(\mathfrak{G})].$$

**引理 4**  $\tilde{S}^n$  与  $Z$  即  $\mathfrak{C}(\rho(G))$  一致<sup>②</sup>。

**証明** 一般, 假如  $GL(V^n) \ni v = (\alpha_{ij}^{(i)})$ , 由例 3 得

$$\rho(x) \cdot (\alpha_{ij}^{(i)}) = (\alpha_{ij}^{(x^{-1}(i))}), \quad (\alpha_{ij}^{(i)}) \cdot \rho(x) = (\alpha_{x(i)j}^{(i)}).$$

但 
$$\alpha_{ij}^{(x^{-1}(i))} = \alpha_{x(i)j}^{(i)} \Leftrightarrow \alpha_{ij}^{(i)} = \alpha_{ij}^{(x^{-1}[x(i)])} = \alpha_{x(i)j}^{(i)},$$

因此  $v \in Z \Leftrightarrow v \in \tilde{S}^n$ . 所以  $\tilde{S}^n = Z$ . (証毕)

由引理 3, 4 (把  $\tilde{S}^n$  作为媒介), 因为  $Z = [\sigma^n(\mathfrak{G})]$ , 于是命題 55 得証。把以上作为准备, 即得我們的目标关于  $\mathfrak{G}$  的表現  $\sigma^n$  的定理 34。

<sup>①</sup> 在这引理中  $\tilde{S}^n, \sigma^n(\mathfrak{G})$  都是看成为向量空間  $\mathfrak{L}(V^n)$  中的向量。为了与引理 1 比較, 可参考下面的对应。

$$\begin{array}{ccccccc} \text{引理 1:} & V^n & S^n & \rho(x) & \underbrace{u \otimes \cdots \otimes u}_{n \text{ 个}} & u \in V \\ & \downarrow & \downarrow & \downarrow & \downarrow & \\ \text{引理 3: } \mathfrak{L}(V^n) = (\mathfrak{L}(V))^n & \tilde{S}^n & \tilde{\rho}(x) & \underbrace{A \otimes \cdots \otimes A}_{n \text{ 个}} & A \in \mathfrak{L}(V) \end{array}$$

在引理 1 中对于任意  $u \in V$ , 集合  $\{u \otimes \cdots \otimes u\}$  中每个元显然对  $\rho(x)$  ( $x \in S_n$ ) 不变, 因此它含于  $S^n$ . 然后再証明它的綫性包絡和  $S^n$  的綫性包絡相等。

在引理 3 中对于任意  $A \in \mathfrak{L}(V)$ , 集合  $\{A \otimes \cdots \otimes A\}$  就是  $\sigma^n(\mathfrak{G})$ , 而它的每一元  $z, z = \underbrace{A \otimes \cdots \otimes A}_{n \text{ 个}}$ , 如果  $A = (a_{kl}^j)$  ( $j, k = 1, 2, \dots, n$ ), 那末矩陣  $z$  中的元一般是

$a_{k_1 \dots k_n}^{j_1 \dots j_n} \dots a_{k_n}^{j_n}$ , 記为  $\alpha_{(l)}^{(i)}$  ( $l = (j_1 \dots j_n), i = (k_1 \dots k_n)$ ), 于是对于任意  $x \in S_n$ , 显然  $\alpha_{(l)}^{(i)} = \alpha_{(l)}^{(i)}$ . 所以向量  $z = (\alpha_{(l)}^{(i)})$  含于  $\tilde{S}^n$ . 同样可証明  $\sigma^n(\mathfrak{G})$  也含于  $\tilde{S}^n$ . 因此用引理 1 的同样証法可以証明  $\tilde{S}^n$  与  $\sigma^n(\mathfrak{G})$  的綫性包絡一致。——譯者注

<sup>②</sup> 在这引理中是将  $\tilde{S}^n, \sigma^n(\mathfrak{G}), \rho(x)$  看成为向量空間  $V^n$  上的綫性变换。——譯者注



**定理 34** (1) 假定  $V$  是把  $C$  作为基础体的  $m$  維向量空間,  $\mathfrak{G} = GL(V)$  的自然表現是  $\sigma$ , 那末把  $V^n$  作为表現空間的  $\mathfrak{G}$  的表現  $\sigma^n$  是完全可約的。

(2) 假如  $n$  阶对称群  $G = \mathfrak{S}_n$  把  $V^n$  作为表現空間的表現  $\rho$  由 (43.1) 定义, 那末  $\sigma^n$  的既約子表現的表現空間的全体, 如果对应于行数是小于或等于  $m$  的  $G$  的盘  $B$  的 Young 的对称子是  $c_B$  时, 与  $\rho(\hat{c}_B)V^n$  的全体一致。

(3) 为了  $\rho(\hat{c}_{B_1})V^n \sim \rho(\hat{c}_{B_2})V^n$ , 要且只要盘  $B_1, B_2$  是属于同一台。

(4) ((3) 的意义) 对应于台  $D$  的既約表現的重复度等于属于台  $D$  的标准盘的个数  $d_D$ 。

**証明** (1) 在 272 頁中已經証明。

在 (2), 假如  $B$  的行数是  $r$ , 那末只証明  $r > m$  时,  $\rho(\hat{c}_B)V^n = \{0\}$ ,  $r \leq m$  时,  $\rho(\hat{c}_B)V^n \neq \{0\}$  即可。

由引理 2,  $\rho(\hat{c}_B)V^n$  中元关于  $\mathfrak{R}(B)$  是反对称張量。因此关于  $B$  的第一列中元的垂直置換全体又是反对称張量。第一列的垂直置換全体构成  $r$  阶对称群, 假如  $r > m$ , 那末由例 4 反对称張量只是 0。

假如  $r \leq m$ ,  $B$  所属的台是  $D(m_1, \dots, m_r)$  时, 如果

$$V^n \ni v = \underbrace{u_1 \otimes \cdots \otimes u_1}_{\leftarrow m_1 \uparrow} \otimes \underbrace{u_2 \otimes \cdots \otimes u_2}_{\leftarrow m_2 \uparrow} \otimes \cdots \otimes \underbrace{u_r \otimes \cdots \otimes u_r}_{\leftarrow m_r \uparrow},$$

那末  $\rho(\hat{c}_B)V^n \ni \rho(\hat{c}_B)v \neq 0$ 。实际上,

$$\rho(\hat{c}_B)v = \rho(K_B)\rho(H_B)v = [\mathfrak{S}(B):1]\rho(K_B)v,$$

$$\rho(K_B)v = \sum_{k \in \mathfrak{R}(B)} (\text{sgn } k) \rho(k)v \neq 0.$$

(3) 由定理 30 与定理 33 自明。

(4) 因为由前节引理 1,  ${}^{\sharp}V^n$  是两侧理想, 所以能够唯一的分解为  $A$  的最小两侧理想的直和

$${}^n V^* = A^{(1)} \oplus \cdots \oplus A^{(q)}.$$

$A^{(i)} (i=1, \cdots, q)$  能够分解为等于属于对应于它的台  $D^{(i)}$  的标准盘的个数的既約左理想的直和。由这事实与定理 33 (Weyl 的相互律) (4) 是明显的。 (証毕)

**注意 1** 在上面, 只考察了  $A(G)$  的左理想, 即令考察右理想也能够得到与上同样的結果。这时在对应于定理 34 的定理中, 用  $c_B$  代替  $\hat{e}_B$  即可。

**注意 2** 关于对应于台  $D=D(m_1, \cdots, m_r)$  的  $\mathfrak{G}$  的既約表現的級数  $\tilde{d}_D$  下面公式是熟知的 (Weyl)。当  $r < m$  时, 命  $m_{r+1} = \cdots = m_m = 0$ , 設

$$l_i = m_i + m - i \quad (i=1, 2, \cdots, m),$$

$$\Delta(x_1, \cdots, x_m) = \prod_{i < j} (x_i - x_j),$$

則 
$$\tilde{d}_D = \frac{\Delta(l_1, l_2, \cdots, l_m)}{\Delta(m-1, m-2, \cdots, 0)} \quad \textcircled{1}.$$

以上  $\mathfrak{G}$  完全是从代数上来討論, 但若視  $\mathfrak{G}$  为拓扑群, 并且是李 (Lie) 群, 就要考虑  $\mathfrak{G}$  的李环。关于上面  $\mathfrak{G}$  的表現的結果, 自李环論的立場也有意义, 但这让于本丛书中《李群論》一书。又明显的与上类似的結果不仅  $\mathfrak{G} = GL(V)$ , 关于  $\mathfrak{G}$  的各种子群——所謂綫性群, 例如酉群, 旋轉群等——也成立, 对称群的表現論也能够利用这些群的表現論。因为这已經远超过預定的篇幅, 关于这等的詳細討論, 在这里不得不割爱。在本丛书有关群論应用的书中这等事实将会触及。

作为参考书, 一般关于代数, 在 §2 曾举出的 van der Waerden 的书在今天仍是标准的著作之一。但关于对偶空間和張量积等沒有象本书那样的处理。关于綫性代数方面其詳有 N. Bourbaki 的

① 参考 H. Weyl: The Classical Groups (1939), Chapter VII. 5. —譯者注

綫性代数 (Algèbre Linéaire), 多重綫性代数 (Algèbre Multilinéaire) 两分册。

关于群的表現論有 H. Weyl 古典的“群論与量子力学”(有內山氏日譯本)。关于 § 42 的內容也同样出現于 Weyl 的古典群論 (Classical Groups)。但敘述得不容易理解。van der Waerden 的量子力学中的群論方法 (Die gruppentheoretische Methode in der Quantenmechanik (1932)) 有更詳解說。H. Boerner 的群表示論 (Darstellungen von Gruppen (1955)) 引入新的結果, 其闡述就清楚多了。

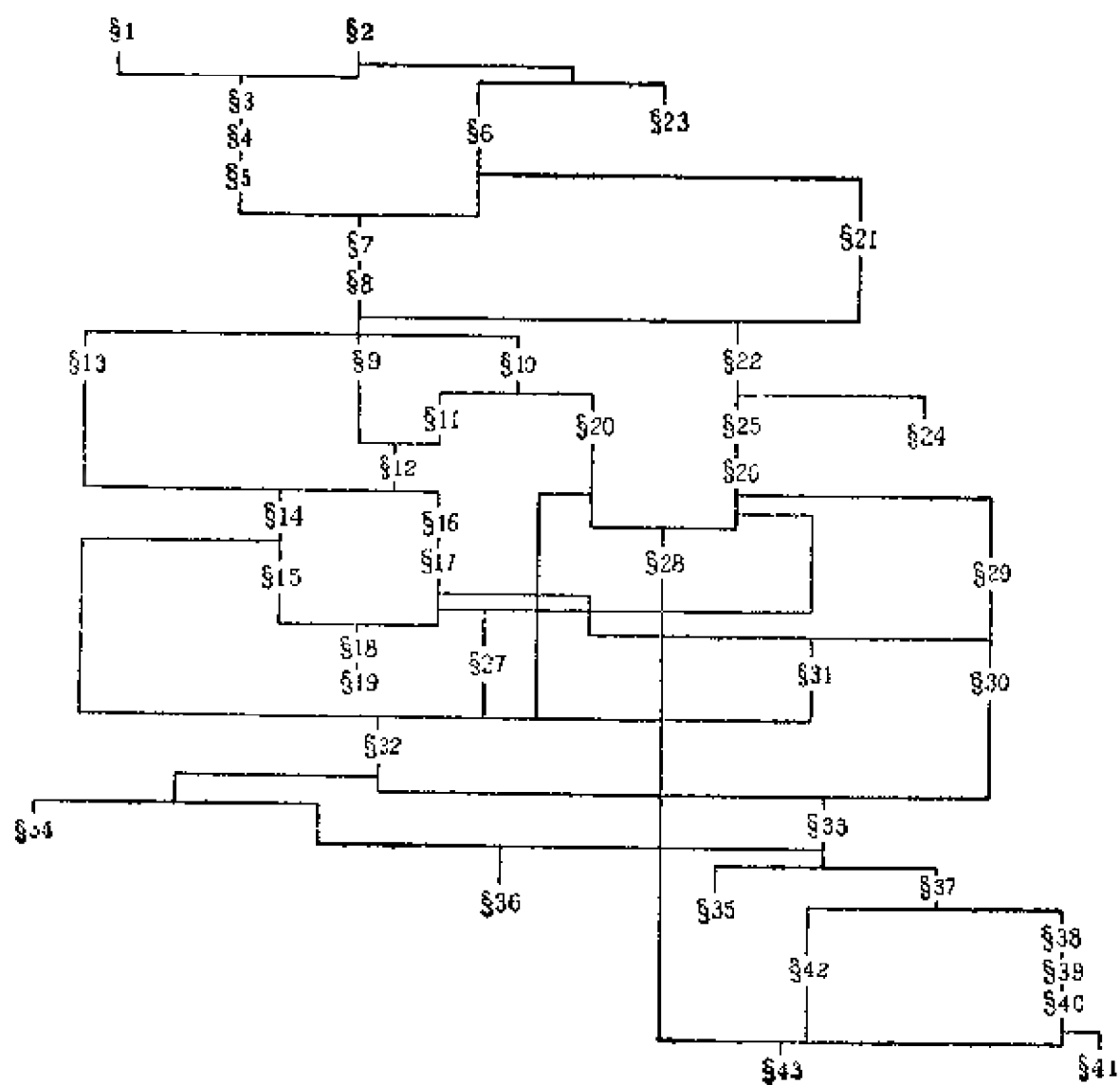
最后就本书执笔的責任置一言。在本册不采取依照章节执笔的方針。最初两个笔者討論全部的結構, 杉浦就全体作出第 1 次原稿, 弥永把它整理, 因此关于錯誤遺漏的責任弥永不得不多担負些。時間不充裕, 整理不充分, 加之在前两章上又出現了明显錯排<sup>①</sup>。这回明显的遺漏恐也不免, 希望讀者指正。

又在整理阶段, 布川正巳君謄清原稿并提供許多宝贵意見, 因此得到改善的地方不少。謹記感謝之意。

---

① 翻譯時已予校正。——譯者注

为便利讀者,把各节之間的邏輯关系列成图表如下:



## 附录 有限旋轉群\*

3 維 Euclid 空間中剛体运动一般由平移及旋轉結合而成，且我們在几何中很容易証明使空間中一点  $O$  不动的剛体运动一定是一旋轉。因此(均以  $O$  点不动，下同)两旋轉的乘积及一旋轉的逆皆仍为旋轉，故所有旋轉成一群。下面研究此群的具有若干种不同构造的有限子群。

今以  $O$  点为中心作一单位球面  $\mathbb{S}$ ，每一旋轉决定  $\mathbb{S}$  自身上的点与点間的一个一一对应，且决无两不同的旋轉决定  $\mathbb{S}$  上相同的对应，故要研究所有的旋轉只要研究  $\mathbb{S}$  上如此的对应——我們仍叫它做旋轉——好了。

以后  $\mathbb{S}$  上的点用大写拉丁字母表示， $\mathbb{S}$  上的旋轉用小写的希腊字母表示。

空間一旋轉若非不动运动(以  $1$  表示)就使通过  $O$  点的某一直綫上每一点不动，因此  $\mathbb{S}$  上任一旋轉  $\sigma$  若  $\neq 1$ ，必使  $\mathbb{S}$  上两直徑对頂点  $P, P'$  不动。此两点称为  $\sigma$  的极，如  $P$  已定，它的直徑对頂点  $P'$  也唯一决定。故任一旋轉如以  $P$  为极，則亦非以  $P'$  为极不可。

我們都知道对一旋轉  $\sigma$ ，必有一“旋轉角”  $\varphi_\sigma$  ( $0 \leq \varphi_\sigma < 2\pi$ ) 与它对应。若  $\sigma, \tau$  有相同的极，則

$$\varphi_{\sigma\tau} \equiv \varphi_\sigma + \varphi_\tau \pmod{2\pi}. \quad (1)$$

以上皆为旋轉的基本性质。我們現在假定  $\mathbb{G}$  是  $\mathbb{S}$  的一有限子群，含有  $N (> 1)$  个  $\mathbb{S}$  上的旋轉，有限群的存在是不成問題的。

---

\* 1951 年武汉大学数学系代数教学小組在四年級集体开“群論”进修課，用 H. Zassenhaus 著 *Lehrbuch der Gruppentheorie* 为教本，該书叙述过簡，論証亦不詳，教学双方，均感困难，因此小組着手根据該书編譯，由各主讲人执笔，此文系路見可同志根据該书第 1 章 § 6 編譯的。

我們想知道  $\mathfrak{G}$  有几种不同的构造, 必須先了解与它有关的几个基本性质。

球面上已知两定点  $P, Q$ , 如  $\mathfrak{G}$  中有一  $\sigma$  存在使  $\sigma P = Q$ , 則称  $P$  与  $Q$  (关于  $\mathfrak{G}$ ) 为共轭的。立刻可以看到共轭关系是等价关系, 故球面上的点分成了若干共轭类。我們如只考虑所有  $\mathfrak{G}$  中旋轉的极所成的 (有限) 集合, 則它也因此分成有限个共轭类:

$$\mathfrak{P}_1, \mathfrak{P}_2, \dots, \mathfrak{P}_H.$$

每一类  $\mathfrak{P}_i$  中的  $p_i$  个极都是共轭的, 且不同类中的极也不共轭。

在  $\mathfrak{G}$  中任取一旋轉的极  $P$ , 則  $P$  必属于上述某一类。設

$$P \in \mathfrak{P}_i \subseteq \mathfrak{P},$$

$\mathfrak{P}$  中連  $P$  在內共有  $p - p_i$  个极  $P_1, P_2, \dots, P_p$  (其中有一个就是  $P$ )。今考虑  $\mathfrak{G}$  中所有使  $P$  不动的旋轉 (即以  $P$  为极的旋轉加上  $\mathbf{I}$ ), 这些旋轉形成一群  $\mathfrak{g}_P \subseteq \mathfrak{G}$ 。因为每一  $P_j (j=1, \dots, p)$  与  $P$  共轭, 故有一  $\sigma_j \in \mathfrak{G}$  存在, 使

$$\sigma_j P = P_j \quad (j=1, \dots, p).$$

对  $\mathfrak{G}$  的任一旋轉  $\sigma$ , 因  $\sigma P$  与  $P$  共轭, 故必对某一  $k (1 \leq k \leq p)$ ,

$$\sigma P = P_k = \sigma_k P,$$

因此

$$\sigma_k^{-1} \sigma P = \mathbf{I} P = P,$$

即  $\sigma_k^{-1} \sigma \in \mathfrak{g}_P$  或  $\sigma \in \sigma_k \mathfrak{g}_P$ 。故所有  $\mathfrak{G}$  的元自  $\mathfrak{g}_P$  出发分成  $p$  个右剩余类:

$$\mathfrak{G} = \{\sigma, \mathfrak{g}_P, \sigma_2 \mathfrak{g}_P, \dots, \sigma_p \mathfrak{g}_P\}.$$

这些剩余类由  $p$  完全决定。 $\mathfrak{g}_P$  本身亦为剩余类之一, 每一剩余类含有

$$n = \frac{N}{p} \quad (\text{一般 } n_i = \frac{N}{p_i}, i=1, \dots, H) \quad (2)$$

个元。 $P$  点称作  $\mathfrak{G}$  中的一个  $n$  回极, 因为  $n$  由  $N$  与  $p$  决定, 所以  $\mathfrak{P}$  中每一点都是  $n$  回极。且由此可見若  $\sigma$  以  $P$  ( $n$  回极) 为极, 則

必  $\sigma^n = I$ ; 因  $\sigma \in \mathfrak{g}_P$  而  $\mathfrak{g}_P$  既將  $\mathfrak{G}$  分成  $p$  个右剩余类, 它的級 (元数) 非是  $n$  不可。注意  $n$  必須大于 1, 因若  $n=1$  則  $\mathfrak{g}_P = I$ ,  $P$  便不是极了。

設  $\tau$  是  $\mathfrak{G}$  中任一元。我們已見由  $P$  得导出  $\mathfrak{g}_P$ , 現在問由  $\tau P$  导出的  $\mathfrak{g}_{\tau P}$  是什么?  $\tau P$  既与  $P$  共轭, 故亦为一  $n$  回极, 因此  $\mathfrak{g}_{\tau P}$  的級也是  $n$ 。但这我們还嫌不够, 今將証明

$$\mathfrak{g}_{\tau P} = \tau \mathfrak{g}_P \tau^{-1}. \quad (3)$$

設  $\sigma_1 \in \mathfrak{g}_{\tau P}$ , 即  $\sigma_1 \tau P = \tau P$ , 故  $\tau^{-1} \sigma_1 \tau P = P$ , 因之  $\tau^{-1} \sigma_1 \tau \in \mathfrak{g}_P$ , 或  $\sigma_1 \in \tau \mathfrak{g}_P \tau^{-1}$ , 所以  $\mathfrak{g}_{\tau P} \subseteq \tau \mathfrak{g}_P \tau^{-1}$ 。

反之, 設  $\sigma \in \mathfrak{g}_P$  即  $\sigma P = P$ , 故  $\tau \sigma \tau^{-1}(\tau P) = \tau P$ , 或  $\tau \sigma \tau^{-1} \in \mathfrak{g}_{\tau P}$ , 所以  $\tau \mathfrak{g}_P \tau^{-1} \subseteq \mathfrak{g}_{\tau P}$ 。(3) 告成立。

用群論的術語言,  $\sigma_1 = \tau \sigma \tau^{-1}$  与  $\sigma$  互为共轭;  $\mathfrak{g}_{\tau P}$  与  $\mathfrak{g}_P$  互相共轭。故 (3) 的意义是: 由共轭的极导出  $\mathfrak{G}$  的共轭子群。

今研究  $\mathfrak{G}$  中旋轉数 ( $N$ ) 与极的总数間有怎样的关系?

任一使  $n$  回极  $P$  不动的旋轉有  $n$  个, 其中有一个为  $I$ , 故  $\neq I$  的有  $n-1$  个, 即以  $P$  为极的有  $n-1$  个。故在  $\mathfrak{P}$  类中以任一点为极的旋轉 ( $\neq I$ ) 共有  $p(n-1)$  个; 因为任一与  $P$  共轭的极  $Q$  也是  $n$  回极, 而以  $Q$  为极的旋轉 ( $\neq I$ ) 也有  $n-1$  个。故  $\mathfrak{G}$  中极的总数有

$$\sum_{i=1}^H p_i (n_i - 1)$$

个。但如有若干个旋轉以同一点为极, 該极仍計算为若干次, 不合并。另一方面,  $\mathfrak{G}$  中共有  $N-1$  个  $\neq I$  的旋轉, 每一旋轉有两极, 故

$$2(N-1) = \sum_{i=1}^H p_i (n_i - 1).$$

两边以  $N$  除之, 注意  $N = p n_i$ , 得

$$2\left(1 - \frac{1}{N}\right) = \sum_{i=1}^H \left(1 - \frac{1}{n_i}\right). \quad (4)$$

因  $N > 1$ , 故

$$2 > 2\left(1 - \frac{1}{N}\right) \geqslant 1. \quad (5)$$

又因  $n_i \geqslant 2$ , 故

$$\begin{aligned} 1 &> 1 - \frac{1}{n_i} \geqslant \frac{1}{2}, \\ H &> \sum_{i=1}^H \left(1 - \frac{1}{n_i}\right) \geqslant \frac{H}{2}. \end{aligned} \quad (6)$$

欲(4)成立, 因(5)的关系, 由(6)知  $H = 2$  或 3。

I. 若  $H = 2$ , 即

$$\frac{2}{N} = \frac{1}{n_1} + \frac{1}{n_2},$$

但因

$$2 \leqslant n_i \leqslant N, \quad (7)$$

故非  $n_1 = n_2 = N$  不可。

II. 若  $H = 3$ , 則

$$\frac{2}{N} = \frac{1}{n_1} + \frac{1}{n_2} + \frac{1}{n_3} - 1. \quad (8)$$

令  $n_1 \leqslant n_2 \leqslant n_3$ , 即  $1/n_1 \geqslant 1/n_2 \geqslant 1/n_3$ . 若  $n_1 \geqslant 3$ , 則

$$1/n_1 \leqslant 1/3,$$

故(8)式右边为負数, 不可能; 故必  $n_1 = 2$ , 因之(8)成为

$$\frac{2}{N} = \frac{1}{n_2} + \frac{1}{n_3} - \frac{1}{2}. \quad (8')$$

如  $n_2 > 4$ , 則  $1/n_2, 1/n_3$  均  $< 1/4$ , (8') 右边又为負数, 不可能; 故  $n_2 \leqslant 3$ . 因此又可分成下列数种情形:

$$\text{a) } n_2 = 2, \text{ 則 } n_3 = \frac{N}{2},$$



- b)  $n_2 = n_3 = 3$ , 則  $N = 12$ ,  
 c)  $n_2 = 3, n_3 = 4$ , 則  $N = 24$ ,  
 d)  $n_2 = 3, n_3 = 5$ , 則  $N = 60$ ,  
 e)  $n_2 = 3, n_3 \geq 6$ , 則 (8') 右边又为負数, 又不可能。

今分述在上列諸情形下  $\mathfrak{G}$  的构造形式。

I.  $H = 2, n_1 = n_2 = N (> 1)$ .

此时  $\mathfrak{P}_1$  及  $\mathfrak{P}_2$  中各含一个极, 各与自己共轭。故  $\mathfrak{G}$  中所有旋轉 ( $\neq I$ ) 有相同的两极。設  $\mathfrak{G}$  中有最小正旋轉角的旋轉为  $\sigma$ , 其旋轉角为  $\varphi_\sigma (> 0)$ .  $\mathfrak{G}$  中任一旋轉  $\tau$  如有旋轉角  $\varphi_\tau$ , 則必有一整数  $m$  存在, 使

$$m\varphi_\sigma \leq \varphi_\tau \leq (m+1)\varphi_\sigma,$$

但因  $\varphi_{\sigma^{-1}} = -\varphi_\sigma$ ,  $\varphi_{\sigma^m} = m\varphi_\sigma$ , 故

$$0 \leq \varphi_{\sigma^{-m}\tau} < \varphi_\sigma.$$

$\varphi_\sigma$  既为最小正旋轉角, 故  $\varphi_{\sigma^{-m}\tau} = 0$ , 即  $\varphi_\tau = \varphi_{\sigma^m}$  或  $\tau = \sigma^m$  (参看 (1)). 故此时  $\mathfrak{G}$  为一  $N$  阶的循环群, 以  $Z_N$  表示。

由这一类旋轉群的分析可得下列几条重要的結果:

1° 由  $P$  为一  $n$  回极, 則  $\mathfrak{G}$  中凡使  $P$  不动的旋轉形成的群  $\mathfrak{G}_P$  (已見其有  $n$  个元) 为一  $n$  阶循环群。因  $\mathfrak{G}_P$  本身也是一有限群, 它必属上述諸形之一, 但  $\mathfrak{G}_P$  中一切旋轉使  $P$  不动, 故  $P$  与自身共轭, 即  $P$  所属的共轭类  $\mathfrak{P}_1$  只有  $p_1 = 1$  个元, 故  $n_1 = n/1 = n = \mathfrak{G}_P$  的元数。上列諸款中只有 I 可能有这样的情形 [II. a) 中  $N \neq 2$ , 因否則  $n_3 = 1$  了]。

故  $\mathfrak{G}_P$  为一  $n$  阶循环群。

2° 若  $\sigma, \tau$  为  $\mathfrak{G}$  中以  $P$  为极的两旋轉, 則必以同样另一点  $P'$  为极;  $P'$  称为  $P$  的直径对顶点 (几何的看法見前)。

因由  $\sigma, \tau$  可生成一有限循环群, 又必須为  $I$  的样子;  $Z_m$ , 而  $n_1 = n_2 = M$ ,  $Z_m$  中仅有两极, 故除  $P$  外只有一个极了。

3°  $\mathfrak{G}$  中一对直径对顶极点  $P, P'$  的回数相同——显然。

4° 若  $P, P'; Q, Q'$  为两对直径对顶极点, 且  $\mathfrak{G}$  中有一  $\tau$  使  $\tau P = Q$ , 則必  $\tau P' = Q'$ .

設  $\mathfrak{G}$  中旋轉  $\sigma$  以  $P, P'$  为极,  $\rho$  以  $Q, Q'$  为极, 則

$$\tau\sigma\tau^{-1}Q = Q,$$

即  $\tau\sigma\tau^{-1}$  的极为  $Q$ , 故由 2°, 亦以  $Q'$  为极:

$$\tau\sigma\tau^{-1}Q' = Q',$$

或

$$\sigma(\tau^{-1}Q') = \tau^{-1}Q',$$

故  $\sigma$  以  $\tau^{-1}Q'$  为极。但显然  $\tau^{-1}Q' \neq P$ , 故  $\tau^{-1}Q' = P'$  即  $\tau P' = Q'$ .

有了这些性质再研究 II 的情形, 就方便得多了。

II<sub>a</sub>.  $H=3, n_1=n_2=2, n_3=N/2$  ( $N>2$ ).

$\mathfrak{P}_3$  中有两个  $N/2$  回极  $P, P'$  互为共轭。以  $P$  为极的旋轉必使  $P$  不动, 但  $P'$  为唯一与  $P$  共轭的极, 故  $P'$  亦不动。即  $P'$  非为  $P$  的直径对顶点不可。故  $\mathfrak{g}_P = \mathfrak{g}_{P'} = \mathfrak{g}$ . 因此  $\mathfrak{G}$  可分成两个右剩余类 (因  $p=2$ )

$$\mathfrak{G} = \{\mathfrak{g}, \tau\mathfrak{g}\},$$

其中  $\tau \notin \mathfrak{g}$ , 我們將  $\tau$  取定不再更改。

因  $P, P'$  为  $\mathfrak{P}_3$  中仅有的两共轭极, 故  $\mathfrak{G}$  中任一旋轉或使  $P', P$  不动, 或使它們互換。若  $\sigma \in \mathfrak{G}$ , 則必  $\sigma P = P', \sigma P' = P$ , 故  $\sigma^2 P = P$ , 因此  $\sigma^2 = I$  (因  $\sigma$  有极, 故  $\sigma^2$  亦使此两极不动, 今又使  $P$  不动, 故  $\sigma^2 = I$ . 此一推理法以下常用)。  $\tau$  既不属于  $\mathfrak{g}$ , 故  $\tau^2 = I$ . 对任一  $\sigma \in \mathfrak{g}$ , 亦必  $(\tau\sigma)^2 = I$ . 故

$$\tau\sigma = (\tau\sigma)^{-1} = \sigma^{-1}\tau^{-1} = \sigma^{-1}\tau. \quad (9)$$

$\mathfrak{G}$  由  $\mathfrak{g}$  及  $\tau\mathfrak{g}$  构成。  $\mathfrak{g}$  由  $1^\circ$  为  $-N/2$  阶循环群,  $\mathfrak{g}$  中两元的乘积自然很容易决定。設  $\mathfrak{g}$  的元写成  $\sigma_1, \sigma_2, \dots$ , 則  $\tau\mathfrak{g}$  的元为

$$\rho_1 = \tau\sigma_1, \rho_2 = \tau\sigma_2, \dots,$$

但

$$\rho_i\sigma_j = (\tau\sigma_i)\sigma_j = \tau(\sigma_i\sigma_j).$$

又由(9)式

$$\begin{aligned}\sigma_i \rho_j &= \sigma_i (\tau \sigma_j) = (\sigma_i \tau) \sigma_j = \tau (\sigma_i^{-1} \sigma_j), \\ \rho_i \rho_j &= (\tau \sigma_i) (\tau \sigma_j) = \tau (\sigma_i \tau) \sigma_j = \tau^2 \sigma_i^{-1} \sigma_j = \sigma_i^{-1} \sigma_j.\end{aligned}$$

故  $\mathfrak{G}$  中任意两元的积可写成  $\sigma_k$  或  $\rho_k$  的样子。因此  $\mathfrak{G}$  的群表(乘法表)完全可写出,亦即  $\mathfrak{G}$  的构造完全决定。这种  $\mathfrak{G}$  以  $D_N$  表示,叫做**两面体群**(几何意义见后,下同)。

$$\text{II}_b. \quad H=3, \quad n_1=2, \quad n_2=n_3=3, \quad N=12.$$

$\mathfrak{P}_3$  中含有四个共轭 3 回极  $A, B, C, D$ 。  $\mathfrak{G}$  中任一旋轉将此四极点互换, 故可使  $\mathfrak{G}$  中任一旋轉  $\sigma$  与  $A, B, C, D$  所成的置换群  $\mathfrak{S}_4$  中某一元对应。

$\mathfrak{G}$  中决无  $\sigma$  与  $\mathfrak{S}_4$  中如  $(A B C D)$  形者对应(即  $\sigma A=B, \sigma B=C, \dots$ ), 因否则  $\sigma$  的极将为 4 回极了, 但  $\mathfrak{G}$  中无这种极,  $\mathfrak{G}$  中亦无  $\sigma$  与如  $(A B)(C D)$  形者对应, 因否则  $\sigma$  以  $C, D$  为极且  $\sigma^2=I$  故  $C, D$  将为 2 回极, 故  $\mathfrak{G}$  中旋轉的对应元在交代群  $\mathfrak{A}_4$  内。

上述对应虽然使旋轉的乘积对应于置换的乘积, 逆对应于逆, 因此这种对应实为一同态。又  $\sigma \neq I$  决不可能使  $A, B, C, D$  都不动, 即只有  $I$  对应于不动置换, 因此不同的旋轉对应于不同的置换。

$\mathfrak{A}_4$  有 12 个置换而  $\mathfrak{G}$  亦有 12 个旋轉, 故  $\mathfrak{G}$  与  $\mathfrak{A}_4$  的构造同。即  $\mathfrak{G} \simeq \mathfrak{A}_4$ 。此时  $\mathfrak{G}$  称为**四面体群**。

$$\text{II}_c. \quad H=3, \quad n_1=2, \quad n_2=3, \quad n_3=4, \quad N=24.$$

考虑  $\mathfrak{P}_2$  中的八个 3 回极, 因其他共轭类中无 3 回极, 故此八点为四对直径对顶点:

$$a: A, A'; \quad b: B, B'; \quad c: C, C'; \quad d: D, D'.$$

$\mathfrak{G}$  中任一旋轉  $\sigma$  必使此四对顶点对与对间互换(由  $4^\circ$ ), 例如  $\sigma$  使  $(abc)(d)$ , 意即  $\sigma a=b, \sigma b=c, \sigma c=a, \sigma d=d$ , 但  $\sigma A$  可能为  $B$  亦可能为  $B'$  及  $\sigma D$  可能为  $D$  亦可能为  $D'$ 。

今将証明若  $\sigma \in \mathfrak{G}$  使  $(a)(b)(c)(d)$ , 则必  $\sigma=I$ 。因若  $\sigma \neq I$

且使 (a) (b) (c) (d), 則  $\sigma$  不可能使两对或两对以上的頂点都不动, 故  $\sigma$  只有两种可能的样子:

1)  $\sigma$  使  $(AA')(BB')(CC')(D)(D')$ ,

2)  $\sigma$  使  $(AA')(BB')(CC')(DD')$ .

若  $\sigma$  为属于 1) 的样子, 即  $D, D'$  为它的极, 但  $\sigma^2 = I$ , 故  $D, D'$  将为 2 回极, 与所設相反。

若  $\sigma$  属于 2) 的样子, 則任取一  $\tau (\neq I) \in \mathfrak{G}$ , 則  $\tau A, \tau A'$  必为  $a, b, c, d$  中某一对极, 但

$$\tau\sigma\tau^{-1}(\tau A) = \tau A', \quad \tau\sigma\tau^{-1}(\tau A') = \tau A,$$

即  $\tau\sigma\tau^{-1}$  亦为互換  $\tau A, \tau A'$ , 同样它亦互換  $\tau B, \tau B'$  等, 所以  $\tau\sigma\tau^{-1}$  与  $\sigma$  有同样的性质, 而  $\sigma\tau\sigma\tau^{-1}$  使此八极皆不动, 故

$$\sigma\tau\sigma\tau^{-1} = I,$$

或

$$\tau = \sigma\tau\sigma.$$

$\tau$  既为任意, 今取以  $A, A'$  为极的一旋轉  $\tau$ , 則  $\sigma\tau$  将  $A, A'$  互換, 故又有  $\sigma\tau\sigma\tau = I$  或  $\tau^{-1} = \sigma\tau\sigma$ , 与前一結果相較, 得  $\tau = \tau^{-1}$  或  $\tau^2 = I$ , 因此  $A, A'$  为 2 回极亦与所設相反, 所以  $\sigma$  非为  $I$  不可。

若  $\sigma_1, \sigma_2$  为  $\mathfrak{G}$  中两旋轉皆使  $a, b, c, d$  有同样的置换, 因此  $\sigma_1\sigma_2^{-1}$  就使 (a) (b) (c) (d), 故必  $\sigma_1\sigma_2^{-1} = I$ , 或  $\sigma_1 = \sigma_2$ .

于是  $\mathfrak{G}$  中任一旋轉必与  $a, b, c, d$  間一个置换对应, 且不同旋轉对应于不同置换, 而  $\mathfrak{G}$  与  $\mathfrak{S}_4$  皆含有 24 个元。同  $\Pi_6$  之理, 必  $\mathfrak{G} \cong \mathfrak{S}_4$ . 这种  $\mathfrak{G}$  称为 (六面体或) 八面体群。

$$\Pi_4. \quad H=3, \quad n_1=2, \quad n_2=3, \quad n_3=5, \quad N=60.$$

考虑  $\mathfrak{P}_1$  中 30 个 2 回极, 以同上的理由共成十五对直径对頂点。

設  $p: P, P'$  为其中一对, 以  $P, P'$  为极的旋轉只有一个  $\sigma (\neq I)$ , 当然  $\sigma^2 = I$ , 又因  $P, P'$  共轭, 故必有一  $\tau$  存在, 使  $\tau P = P'$ ,

因此  $\tau P' = P$ ; 也有  $\tau^2 = I$ , 今証下列諸性质:

1.  $\mathcal{G}$  中使  $(p)$  不变 (即使  $P, P'$  不动或彼此互換) 的旋轉只有  $\sigma, \tau, \rho = \sigma\tau, I$  四个。

2.  $\mathcal{G}$  中与  $\sigma$  交換可能的旋轉亦仅有  $\sigma, \tau, \rho, I$  四个。

3. 設  $\tau$  的极为  $q: Q, Q'$ ;  $\rho$  的极为  $r: R, R'$ ; 則  $\mathcal{G}$  中使  $(q)$  不变或使  $(r)$  不变的旋轉仍是此四个。因之任一旋轉如使  $(p), (q), (r)$  三对中一对不变亦必使其他两对不变。

4. 若此三对极所成的集合叫做  $\mathfrak{p}$ , 則  $\mathcal{G}$  中使  $\mathfrak{p}$  不变的两級旋轉必以三对中某一对为极。

設  $\alpha \in \mathcal{G}$  使  $(p)$  不变, 故

$$\alpha P = P \quad \text{或} \quad \alpha P = P'.$$

若  $\alpha P = P$ , 因为以  $P$  为极的旋轉只有  $\sigma$ , 故  $\alpha = I$  或  $\alpha = \sigma$ . 若  $\alpha P = P'$ , 則  $\alpha\tau^{-1}P = P$ . 同理故  $\sigma\tau^{-1} = I$ , 即  $\alpha = \tau$  或  $\alpha\tau^{-1} = \sigma$  即  $\alpha = \sigma\tau = \rho$ . 故 1 成立。

因  $\rho$  亦將  $P, P'$  互換, 故亦  $\rho^2 = I$ , 即

$$\sigma\tau\sigma\tau = I \quad \text{或} \quad \sigma\tau = (\sigma\tau)^{-1} = \tau^{-1}\sigma^{-1} = \tau\sigma.$$

故  $\sigma$  与  $\tau$  交換可能, 同理  $\sigma, \tau, \rho$  皆互相交換可能。今若  $\alpha \in \mathcal{G}$  与  $\sigma$  交換可能, 即  $\alpha\sigma = \sigma\alpha$ , 故  $\sigma\alpha P = \alpha\sigma P = \alpha P$ , 所以  $\alpha P$  不动。故  $\alpha P$  为  $P$  或  $P'$ , 即  $\alpha$  使  $(p)$  不变, 由 1.,  $\alpha$  只有这几种可能, 故 2. 成立。

$\mathcal{G}$  中使  $q$  不变的旋轉也应有四个, 且此四个为与  $\tau$  唯一交換可能的, 而  $\sigma, \tau, \rho, I$  易見均与  $\tau$  交換可能, 故此四个也非是它們不可。同理对  $\rho$  也是如此。故 3. 成立。

設  $\alpha$  为  $\mathcal{G}$  中一两級旋轉 ( $\alpha \neq I, \alpha^2 = I$ ) 使  $(p)$  不变。由 4°,  $\alpha$  必使  $p, q, r$  三对頂点互換。 $\alpha$  决不可使它們輪換如  $(pqr)$ , 因否則  $\alpha^2 \neq I$  了, 故  $\alpha$  必至少使一对例如  $(p)$  不变。但使  $(p)$  不变的旋轉由 1. 必为  $\sigma, \tau$  或  $\rho$ ; 而此三旋轉分別以此三对点为极。故 4.

亦成立。

$G$  中的 30 个 2 回极因 3. 的緣故, 可以上述的方法分組, 每 6 个一組共有 5 組:

$$p_i = \{p_i: P_i, P'_i; q_i: Q_i, Q'_i; r_i: R_i, R'_i\} \quad (i=1, 2, 3, 4, 5)$$

設以  $p_i, q_i, r_i$  为极的 2 回极旋轉分別为  $\sigma_i, \tau_i, \rho_i$ .

$\mathfrak{G}$  中任一旋轉  $\alpha$  必将整个一組  $p_i$  变成另一組  $p_j$ , 因此每一  $\alpha$  对应于諸  $p_i$  間的一置換, 即  $\mathfrak{S}_5$  的一元。因由 4°,  $\alpha P_i, \alpha P'_i; \alpha Q_i, \alpha Q'_i; \alpha R_i, \alpha R'_i$  仍为此十五对中某三对直徑对頂 2 回极点, 且易見  $\alpha\sigma_i\alpha^{-1}, \alpha\tau_i\alpha^{-1}, \alpha\rho_i\alpha^{-1}$  分別以此三对为极, 而它們間也彼此可以交換可能, 且各不同并异于  $I$ ; 故由性质 2, 它們一定分別是某一組  $\sigma_j, \tau_j, \rho_j$  (次序可顛倒), 亦即:

$$\alpha p_i = p_j.$$

考虑  $\mathfrak{G}$  中所有旋轉使  $p_1$  不变者, 它們形成  $\mathfrak{G}$  的子群  $\mathfrak{g}_1$ . 將  $\mathfrak{G}$  按  $\mathfrak{g}_1$  分成右剩余类, 同一类中的旋轉將  $p_1$  变至同一組  $p_i$ , 且所有各組  $p_i$  中的极点均互相共轭, 故对每一  $p_i$  必有  $\mathfrak{G}$  中旋轉使  $p_1$  变至  $p_i$ . 所以  $\mathfrak{G}$  被分为 5 个右剩余类:

$$\mathfrak{G} = \{\alpha_1\mathfrak{g}_1, \alpha_2\mathfrak{g}_1, \alpha_3\mathfrak{g}_1, \alpha_4\mathfrak{g}_1, \alpha_5\mathfrak{g}_1\} \quad (\alpha_1 = I),$$

因  $\mathfrak{G}$  有 60 个旋轉, 故每一剩余类, 因之  $\mathfrak{g}_1$  含 12 个旋轉。

$\mathfrak{g}_1$  为一 12 元的有限旋轉群, 且它不能为  $I$  或  $\Pi_a$ , 即  $Z_{12}$  或  $D_{12}$  的样子, 因  $\mathfrak{G}$  中因此  $\mathfrak{g}_1$  中无 12 回极亦无 6 回极, 故  $\mathfrak{g}_1$  必为  $\Pi_b$  的样子, 或四面体群, 即

$$\mathfrak{g}_1 \cong \mathfrak{A}_4.$$

与  $\Pi_c$  的情形相仿, 我們將証明  $\mathfrak{G}$  中任一元  $\alpha$  如使  $(p_1), \dots, (p_5)$  都不变, 則必  $\alpha = I$ .

設  $\alpha$  使上述 5 組均不变, 当然  $\alpha \in \mathfrak{g}_1$ , 故若  $\alpha \neq I$  則必为兩級或三級的。  $\alpha$  不能为兩級的, 因若  $\alpha^2 = I$ , 而  $\alpha$  使每一  $p_i$  不变, 故

由性质 4,  $\alpha$  的极将在每一  $p_i$  中, 不可能。今設  $\alpha$  为三級的, 因若  $\alpha^3 = I$ , 且因  $\mathfrak{G}$  中只有 1 个  $n_2$  等于 3. 所以任一三級旋轉  $\beta$  的极  $Q$  必与  $\alpha$  的一极  $P$  共轭, 即有一  $\tau$  存在, 使  $\tau P = Q$ . 但由 (3) 知

$$g_Q = \tau g_P \tau^{-1}.$$

此处  $g_Q = \{I, \beta, \beta^2\}$ ,  $g_P = \{I, \alpha, \alpha^2\}$ . 故  $\beta$  为  $\tau \alpha \tau^{-1}$  或  $\tau \alpha^2 \tau^{-1}$ . 注意  $\alpha$  及  $\beta$  皆使每一  $p_i$  不变, 当然亦使  $\tau^{-1} p_i$  不变, 故

$$\beta p_i = \tau \alpha k \tau^{-1} p_i = \tau \tau^{-1} p_i = p_i \quad (k=1, 2),$$

即  $\beta$  亦使每一  $p_i$  不变, 故所有  $\mathfrak{G}$  中三級旋轉皆使每一  $p_i$  不变, 因之所有三級旋轉皆在  $g_1$  中。但因  $g_1 \cong \mathfrak{A}_4$  仅有 8 个三級元, 而  $\mathfrak{G}$  中已知有  $N/n_2 = 20$  个 3 回极; 这是矛盾的, 不可。所以必定

$$\alpha = I.$$

与前面一样, 由上述結果可推得:  $\mathfrak{G}$  中不同的旋轉对应于不同的  $\{p_i\}$  上的置换。

$\mathfrak{G}$  中决无旋轉对应于如  $(p_1 p_2 p_3 p_4) (p_5)$  或如  $(p_1 p_2 p_3) (p_4 p_5)$  型的置换, 因  $\mathfrak{G}$  中无 4 或 6 回极。

$\mathfrak{G}$  中亦不能有旋轉  $\alpha$  对应于如  $(p_1 p_2) (p_3) (p_4) (p_5)$  型的置换。因为如此, 則  $\alpha^2$  使每一  $p_i$  不动, 故为  $I$ . 因此  $\alpha$  为一兩級旋轉而使  $p_3 p_4, p_5$  皆不动, 按性质 4,  $\alpha$  的极必在此三組的每一組內, 不可能。

所以  $\mathfrak{G}$  中的旋轉皆对应于  $\mathfrak{S}_5$  中的交代群  $\mathfrak{A}_5$ . 而  $\mathfrak{G}$  及  $\mathfrak{A}_5$  各为 60 个元, 故

$$\mathfrak{G} \cong \mathfrak{A}_5.$$

这种  $G$  称作(十二面或)二十面体群。

据上所述, 有限旋轉群仅可能有上列各形式, 但是否每种形式的群确有存在, 尚須証明。实际上, 可用几何方法做出上属各群, 即各群都真实存在, 故本問題获完全解决。

首先, 如 I 型的循环群  $Z_N$  非常容易做成。任取一对直径对頂

点为极，作  $\sigma$  使  $\varphi_\sigma = 2\pi/N$ ，则由  $\sigma$  所生成的即为  $Z_N$ 。

其次，对于最后三型的群恰可分别作球的內接正四面体、正八面体及正二十面体，而使此諸正多面体不变的旋轉所成的群恰分别为此諸群。每一情形下  $\mathfrak{R}_3$  中的极即正多面体的頂点，每一正多面体的每一面的中心形成对偶正多面体的頂点（见图 1）。如以  $O$  点为中心将此諸点射影到球面  $\mathfrak{R}$  上，则成为  $\mathfrak{R}_2$  中的极。如以  $O$  点为中心将多面体的每一棱的中点射影到球面上就成为  $\mathfrak{R}_3$  中的极。每使一正多面体不变的群亦使其对偶正多面体不变。

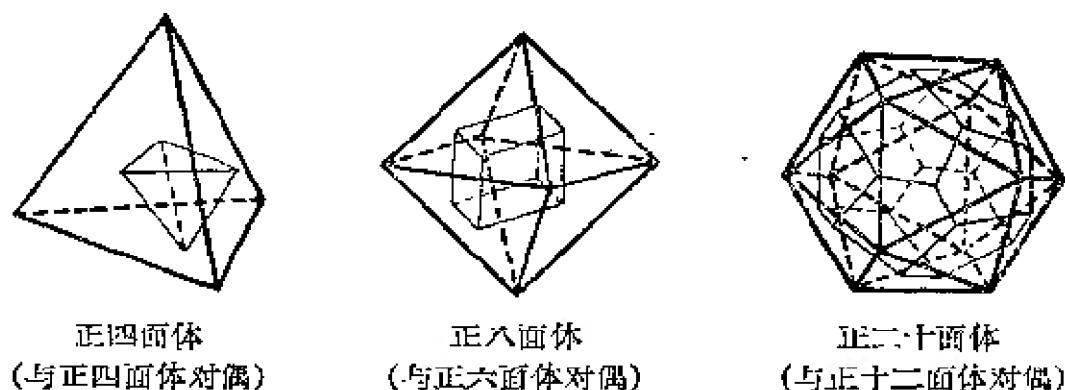


图 1

如图 2 中，二十面体的六个作了記号的棱的中点就与  $\Pi_4$  中的一組  $p$  相似，使这六点不变的群为一四面体群，且它們都是 2 回极，故組成一正四面体的六个棱的中点，亦即一正八面体的六个頂点。

注意正四面体仍与正四面体对偶，与正八面体对偶的为正六面体（正立方体）。如研究使正六面体不变的旋轉群，則与它对偶的又为正八面体，故  $\Pi_6$  亦可称为正六面体群。同理正十二面体与正二十面体对偶，故  $\Pi_{12}$  亦可称为正十二面体群。

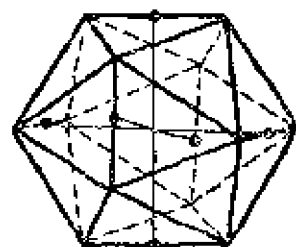


图 2

最后談到  $\Pi_N$  的情形，例如設  $N=6$ ，如图 3，設  $\triangle ABC$  为  $\mathfrak{R}$  上赤道圓的內接正三角形，将此三角形看成“两面体”， $A, B, C$  为



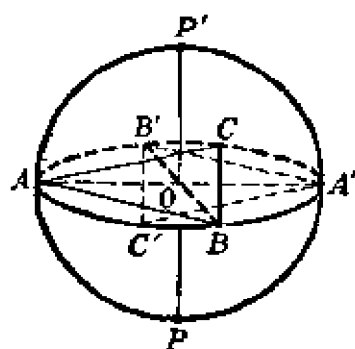


图 3

$\mathbb{R}_2$  中的极点, 自  $O$  作此二重面的垂綫, 将  $\mathbb{R}$  上南北极点  $P, P'$  为  $\mathbb{R}_2$  中的极点, 自  $O$  点与  $\triangle ABC$  各边中点相联, 延长得  $\mathbb{R}_2$  中的三个极点  $A', B', C'$ . 赤道圓上的极点都是 2 回极,  $P, P'$  为 3 回极。每一旋轉均使  $\triangle ABC$  (即正两面体) 不变, 故  $D_6$  的确存在, 并且不妨称它为两面体群。一

般, 只要  $N$  是  $\geq 4$  的偶数, 以同法可証  $D_N$  都存在。事实上,  $D_N$  使赤道圓上一正  $N/2$  边形 ( $N=4$  时任一直徑) 不变。

至此我們对于 3 維 Euclid 空間的有限旋轉群的种类与构造可完全認識了, 它或为由  $\mathbb{R}$  上以一直徑为軸的旋轉  $\sigma\left(\sigma_\varphi = \frac{2\pi}{N}\right)$  所生成 ( $Z_N$ ), 或它的旋轉使一大圓的内接正  $\frac{N}{2}$  边形 ( $N=4$  时为一直徑) 不变 ( $D_N$ ), 或使一内接正多面体不变; 再不然就只含有不动旋轉  $1$ 。